

SECURITY OF MICRO-MAINFRAME LINKS

BY

Tzyy-Hsiung Chai

B.S., National Chung Hsing University, Taiwan, R.O.C., 1980

A MASTER'S REPORT

Submitted in partial fulfillment of the

requirements for the degree

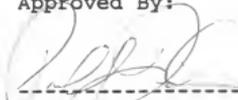
MASTER OF SCIENCE

Department of Computer Science

Kansas State University
Manhattan, Kansas

1987

Approved By:



Major Professor

ACKNOWLEDGEMENT

I wish to express my sincere thanks to Dr. Paul Fisher, my major advisor, who has encouraged me and given me invaluable help. He is a conscientious educator and a dedicated computer scientist with great warm personality.

A special thanks to Dr. Elizabeth Unger and Dr. Rich McBride for acting as my committee members. Also, my thanks to Mrs. Weilin Chen for her indispensable assistance.

After all, I give my heartfelt appreciation to my parents and wife for their love and support.

Table of Contents

	PAGE
Chapter 1. Introduction	1
1.1 Overview	1
1.2 The Basic Problems of Today	3
Chapter 2. Solutions To The Problem	7
2.1 Education Programs for The First Time End-user	7
2.2 Physical Security of Microcomputers	8
2.3 Logical Security of Microcomputers	9
2.4 Telecommunication Security	13
Chapter 3. Encryption Techniques	17
3.1 The DES Algorithm	17
3.2 Survey of Commercial Software Packages	21
3.2.1 P/C Privacy	21
3.2.2 DES-PAC	22
3.2.3 DataSafe	23
3.2.4 PhasorCode 1000	25
3.2.5 SECURE!	26
3.2.6 AutoCrypt I	27
Chapter 4. Other Related Security Concerns	29
4.1 Risk Management	29
4.2 Personnel Security	31
4.3 Contingency Planning	33
Chapter 5. Summary and Conclusions	35
References	37

Appendix:

A. Trademarks	40
B. Selected Sources Of Software	41

Chapter 1. Introduction

1.1 Overview

The introduction of the microcomputer to business and its application as a multifunctional desktop workstation has greatly enhanced the concept of end-user (distributed) computing. As a result of continuous development in the modern electronic technology, microcomputers have become an integral part of the corporate information processing resource. In the beginning, a microcomputer was treated as a toy for the individual who acquired it. However, because of the use over time of the microcomputer, the user view has changed due to the capabilities of the machine. From the basic concept as a toy, the microcomputer has moved to a standalone helpmate. The individual has matured in the use of the microcomputer, and now begins to use it for assistance in performing his/her day-to-day work. The microcomputer at this point has become an extension of one's working tool capabilities, just like the telephone.

While the individual becomes more skilled with his/her standalone system, he/she also notices that the power of microcomputer needs to be expanded. For example, the individual might want a larger disk capacity for the required jobs, and this may require more resources than

most microcomputers can provide. Also, the individual might want to download part or all of an entire database from the mainframe; to upload processed data that resides on a microcomputer to the mainframe database; and to execute a microcomputer-resident program using the data downloaded from the mainframe. Thus, there is a need for a link between the micro and mainframe. With this link, the individual now becomes an end-user who communicates with a corporate database through the medium of the microcomputer.

Nothing is perfect. Inevitably, this link has both advantages and disadvantages. Some of the advantages are the wide variety of permutations and combinations of activity, and the improvement of productivity for the end-user's daily work. One of the disadvantages is the associated, potential security problems. This disadvantage is caused partly by the fact that more "first time" end-users [8] are accessing corporate databases, and partly by the issues inherent in microcomputing. For instance, the possibility that the end-user can expose confidential corporate data is very high, because all of the information is stored on easy-to-carry floppy diskettes. These potential problems are common in any type of configuration of distributed processing. Nevertheless, most of the problems can be resolved by the

software products currently available on the market. A survey of several products was conducted, and the result shows that menu-driven systems and on-line help messages ease users' application of the software package. In addition, the reasonable price of the products and their various functions easily justify users acquisition of the products. This paper attempts to present the security problem in this new environment with some solutions. Also, related security concerns are discussed in order to improve the security of this new environment.

1.2 The Basic Problems Of Today

In this new environment, the central computer site is well protected from security threats; however, the end-user site is not. This is true because current operating systems for microcomputers do not support the high level of security that is present on mainframe computers. Therefore, the majority of the newly introduced security problems are at the microcomputer sites.

There are four existing problems which increase the complexity of securing this link, and they are listed as follows:

First: the proliferation of microcomputers has transformed the person on the micro side of a mainframe link from a data processing professional to a "first time"

computer center manager -- an individual who never before has been responsible for, or even involved with the control of a total computer system[8]. In other words, those new managers are unfamiliar with the types of control needed. Since most of these first time managers do not realize the significance of data control, they often store sensitive, confidential corporate data on floppy diskettes without extra care. When data is downloaded and then modified, they often do not understand the necessity for backups, nor do they understand the problems inherent in duplicated data in terms of consistency. Therefore, many potential security problems are the result of such new processing environments.

Second: in the past, the computer security officer was faced with only the task of securing a large computer installation. Now, with the existence of the individual microcomputers in the offices of an organization, computer security becomes much more complicated, since new knowledge is needed in order to accommodate this change. Nevertheless, most computer security officers have little or no knowledge concerning the microcomputer and its peripherals, the proper handling of floppy diskettes, or that there are, to a limited extent, capabilities available for providing security for such systems.

Third: once numerous microcomputers have been dispersed throughout the organization, there is a lack of information about particular data which is 'floating' around within the organization. The central site concerns involve the downloaded data that might be destroyed or misused by either authorized or unauthorized users. In other words, the central site can exert no control over the information stored on diskettes that was originally mainframe-resident.

Finally: due to the fast-developing technology in modern communication, access to the corporate database is no longer confined to individuals within the corporate premises. Employees can now use those newly-developed communication devices at home to gain access to the corporate database located within the organization. Consequently, this new work environment immediately causes us to focus on some new risks. This is due to the simple fact that we have no control over the corporate information (in electronic form), once it leaves the controlled, corporate premises. Among those risks are: "improper actions by employees of the servicing communications carrier, who may observe, copy, or change messages, or divert them to unauthorized stations; systems failures in the utility switching computers, which could misroute, garble, or destroy information [20]", as well

as the obvious misuse of information by the employee, or those in the home environment.

Chapter 2. Solutions To The Problem

2.1 Education Programs For The First Time End-User

Many first time end-users are often unaware of the importance of computer security. In order to avoid the unnecessary losses of vital information and to achieve the intent of management policies, a well designed first-time, end-user, education program is indeed a must. The objectives of this program would be to ensure that the persons involved are aware of their security responsibilities, the potential risks, and some of the currently available measures that they can take to reduce these potential risks. A further important aspect of this education program is to make the employee aware of the importance of the information which is being manipulated by the micros.

Another similar program is also needed to educate those end-users who already have some computer literacy. It is worthwhile to have these kinds of educational programs in place, because properly trained end-users are usually more productive, and more careful!

Perry [16] suggests that a good education program encompasses the following:

- (1) Formal training programs.
- (2) Training procedures for users of microcomputers.

- (3) Awareness programs for supervisors and managers.
- (4) Security procedures for microcomputer operators.
- (5) Posters/devices posted in the microcomputer area to create an awareness of the need for security.

2.2 Physical Security Of Microcomputers

The microcomputer is itself valuable and therefore must be protected from being sabotaged. Some of the physical security measures can be used to avoid these problems. These include[16]:

- (1) Locking the microcomputer in a secure area.
- (2) Using guards, alarms, and other monitoring devices to detect penetration during nonworking hours.
- (3) Locking areas when employees are absent.
- (4) Using devices to lock the computer to its physical location.
- (5) Putting locks on the computer to turn off power and prevent unauthorized users from having access to the machine.

Once an unauthorized user gains access to a microcomputer, then that user may also gain access to the corporate database. More often than not, this will result in the disclosure of vital information which might lead to a significant loss. Controlling access to a microcomputer

is the first step in overcoming this problem. Today there are some software products, hardware devices or combination of both on the market to meet this need. One of the software products [8] uses the idea that is described as follows: Place the compiled version of the program on every diskette with an AUTOEXEC.BAT file(a file that allows the user to automatically execute commands or programs when MS-DOS is started). When the system is booted , the user is notified that this is a protected diskette. After pressing any key, the user is then requested to enter his or her password. Failure to enter the proper password will cause the bell to ring and the keyboard will lock. Even if the correct password is entered at the outset, the user is requested to answer three personal questions. Failure to do so properly for any question will initiate the alarm sequence. Only after all questions have been correctly answered will the user then be allowed to access the system. Clearly, this scheme is no better than the trust of the individual, and the care with which the individual protects that information. In any security environment, the user always becomes the weak link in the entire process.

2.3 Logical Security Of Microcomputers

Not only is protection of the microcomputer itself

necessary, but we must also be concerned with the protection of data files and programs. The latter is the logical security issues associated with microcomputers. Some of the logical security measures for use with the microcomputer include [9,16]:

- (1) Blanking computer memory before turning off the computer.
- (2) Blanking storage media when no longer needed.
- (3) Security checks on individuals operating the microcomputer.
- (4) Do not leave the microcomputer without logging off of the system.
- (5) Data that is downloaded from the corporate database should be stored on floppy diskettes rather than on the hard disk. This is because floppies can be removed to a more secure place while the hard disk can not.
- (6) Encrypt data that is stored on the diskettes. A simple encryption technique could be for less important data, while a more powerful one could be used for the highest level of secured data.
- (7) Provide added security by requiring "logging in" for a specific program. We can emulate the more sophisticated system by placing appropriate routines

within a special loggon program.

In addition to the above measures, we also need to pay more attention to the handling of diskettes. End-users use diskettes to store information downloaded from the corporate database. As a consequence, diskettes are plentiful and widely dispersed, making inventory and tracking difficult. In addition, diskettes are a primary target for penetration, because they are much easier to carry away than the fixed disks used by a mainframe or a bulky package of computer printouts. Thus, we need to carefully consider the handling of diskettes. There are several controls which we need to consider in order to handle the diskettes properly.

The first one is the adoption of a scheme for classifying information by sensitivity and criticality[24]. This scheme helps to ensure that the data is treated consistently wherever it resides (mainframe,microcomputer), and whatever form it takes(paper, diskettes). Diskettes that contain sensitive information can be separated easily from those containing less sensitive information after a classification scheme has been adopted. In this way, the security officer need not apply stringent controls to all diskettes regardless of the sensitivity of the information each contains.

Secondly, we need to consider the backup issue, since

keeping copies of important files is the best protection against destruction of data. In order to encourage users to perform necessary backup activities, backup procedures should be simple and easy to use. This can be achieved by using a centralized backup procedure, such as having a mainframe keep backup copies of the data resident on a connected microcomputer. Next, individual users should maintain an index of the programs and data files stored on each individual diskette[8]. This indexing could include fields to record, for example, file number, diskette number, date created, data most recently updated, and the author's initials. The purpose of this record would be to provide some insight into the individual files which exist throughout an organization and to avoid time-consuming searches for files, and confusion about which file or diskette is the most recent version.

Finally, we should consider the residues problem[14]. Here, if an area of memory is released by a user or by the system when a file is deleted, the information stored in memory or on the diskettes may remain there, although it is inaccessible in the normal way. With skilled programming, that information can then be read by the next user to whom the space is allocated. It may result in the disclosure of sensitive information if the next user is an unauthorized user such as an industrial spy. Sanitization

can be accomplished by overwriting the area on the diskette with repeated sequences of ones and zeros. In some systems, a diskette reformatting routine can be used to overwrite previously recorded data. In addition, if a diskette which contains sensitive information becomes damaged or worn-out, then it should be destroyed before disposal.

2.4 Telecommunication Security

Since users increasingly access corporate database from remote sites, careful attention must be given to telecommunication security. Communication lines are vulnerable to eavesdropping, or to the insertion of an unauthorized message. " A passive intruder listens to the communication and an active intruder can alter or insert a message [16]." Both types of intrusion can be accomplished through wiretapping, i.e., by physically connecting to a communication path. This brings up the physical security issue of communication lines. The following two requirements might be helpful to the physical security of communication lines[20]:

- (1) Communication cables should be in a conduit or trench whenever the cables are outside of the directly controlled area.

(2) Devices that provide central file storage and units that control communication functions should be secured in restricted areas, where only specially authorized employees can enter.

In addition, user identification/authentication and encryption may be the two most important measures to successfully secure a communications line.

User identification/authentication can be accomplished by requesting a series of passwords or keys from the user making the request to access the system. Once the user gains access to the system, the system should place restrictions on what this user may do. Limitation of what the user can do, once identified and authenticated, is important to control potential damage from unknown parties. To make this measure effective, the selection of passwords (or keys) should be random, should be changed frequently, and should also be long enough to resist an exhaustive trial-and-error attack. This means that systems should allow only few attempts by a user trying to logon before notifying authorities and/or locking the device.

Encryption is probably the most promising control for safeguarding the data on removable storage and communications lines. It is highly recommended that, for

security concerns, data should be encrypted before going out over the communication lines. At this point, encryption can be done in conjunction with other measures, such as compression, packet formation, or check sum calculation. This is called data link encryption [22].

There are three approaches to incorporating encryption into a communications system [12]:

- (1) Link-by-link.
- (2) Node-by-node.
- (3) End-to-end.

In link-by-link encryption, data is encrypted across the medium connecting two directly communicating nodes. Link-by-link encryption is logically independent of the system and does not necessarily imply that the function of encryption is integrated into the communicating nodes. It can be thought of as implemented by a pair of encryption devices bracketing the line between two communicating nodes and their modems.

Node-by-node encryption is logically similar to link-by-link encryption in that each link is protected by a unique key. However the translation from one key to another occurs within a security module, which may be a peripheral device attached to the node. Moreover, plain text occurs only within the security module, not within the node.

In end-to-end encryption, data encrypted at the originating node is not decrypted until it arrives at its final destination. The function of encryption is integrated into the participating nodes to the extent that the system can control the setting of the keys and turning the encryption function on and off. The encryption function to be provided by a host processor node could be provided either by a programmed implementation of the DES algorithm or by special hardware integrated into the central processing unit, into a front-end processor, or into the channel.

Chapter 3. Encryption Techniques

Hopefully, the previous discussion has demonstrated that the encryption technique can be effective and powerful for data both in storage and in transit. By applying the encryption algorithm, one could transform data into an unintelligent form which is useless to unauthorized users. Only authorized users would be able to reconstruct the secretly coded data back into its original, clear form.

The federal encryption standard (Data Encryption Standard) and a survey of some commercial software packages which have an encryption facility will be presented next.

3.1 The DES Algorithm

DES (Data Encryption Standard) is the Federal standard for the encryption algorithm which was issued by the U.S. National Bureau of Standards in 1977. It is a symmetric encryption scheme -- the same key is used for both encryption and decryption. It uses a 64-bit key (of which eight bits are for parity checking) to encrypt 64-bit blocks of plaintext.

The algorithm begins and finishes with a permutation of the 64 bits. In between, there is a series of 16

iterations of complex transformations. A typical iteration is illustrated in Figure 1 [19]. It uses 48 bits of the key in a sequence which is specified in the standard, this is K_n . The right most 32 bits (R_n) of the current version of the transformed input block are expanded to 48 bits by the linear operator (E). These bits are then added modulo 2 to K_n . The resulting 48 bits are divided up into eight six-bit blocks, each of which is transformed by one of the eight s-boxes into a four-bit block. The resulting 32 bits undergo a permutation (P) and are then added modulo 2 to the left most 32 bits (L_n) of the current version of the transformed input block. The two halves are now interchanged to yield the new, current version of the transformed input block.

The original length of key which is selected by the user is 56 bits. To bring the key up to block size, it is artificially expanded to obtain a 64-bit key which is 8 bytes long. As there are over 70,000,000,000,000,000(seventy quadrillion) possible keys of 56 bits and the key can be changed frequently, the threat of someone finding the key can be almost eliminated.

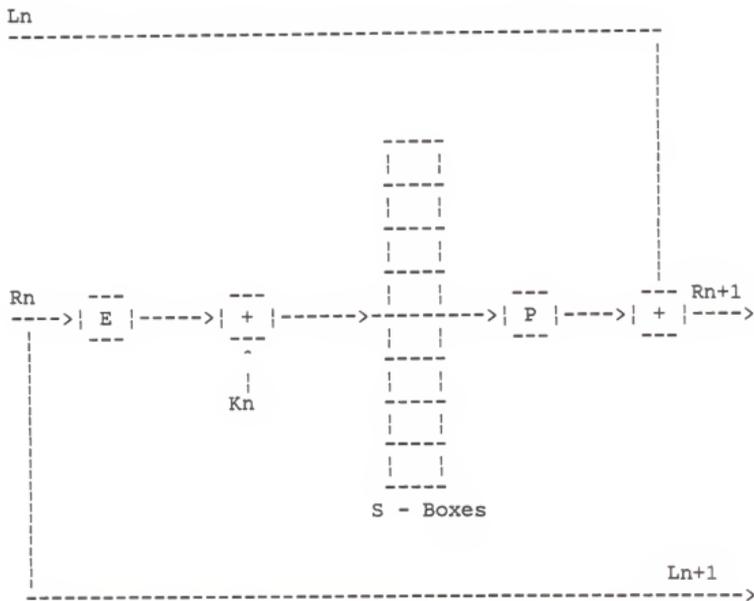


Fig. 1 One of Sixteen Rounds of the DES

The DES algorithm can be applied in two different modes [11]:

1. Electronic Code Book Mode. Data is encrypted using a key in a block of 64 bits. Each block of plain text and encrypted text is independent of preceding and succeeding blocks.
2. Cipher Feedback Mode. The algorithm is used as a

binary stream generator to produce random bits that are combined with binary plain text using the exclusive or logical operator to form binary encrypted text. Input to the algorithm is the previous 64 bits of data that were transmitted or received and as in the alternate mode, a key must be used. Greater security is obtained when this mode is used.

The following quotation outlines the position of the National Bureau of Standards with regard to the implementation of the data encryption standard [1]:

The algorithm specified in this standard is to be implemented in computer or related data communication devices using hardware (not software) technology. The specific implementation may depend on several factors such as the application, the environment, the technology used, etc. Implementations which comply with this standard include Large Scale Integration(LSI) "chips" in an individual electronic package, devices built from Medium Scale Integration(MSI) electronic components, or other electronic devices dedicated to performing the operations of the algorithm. Micro-processors using Read Only Memory(ROM) or micro-programmed devices using microcode for hardware level control instructions are examples of the latter.

From the above, one can see that DES was designed for efficient hardware implementation. Although it has been implemented in software, such implementations do not comply with the standard and are generally inferior in performance to hardware implementation. However, when an organization's need does not justify the hardware

approach, it is possible for that organization to use the DES algorithm to develop its own software product. As mentioned most software encryption is considerably slower than hardware, but software is less costly than hardware considering the initial investment.

3.2 Survey Of Commercial Software Packages

3.2.1 P/C Privacy (The trademark of MCTel)

This package consists of a disk which contains three comparatively short programs. It can be used with floppy and/or hard disk systems as well as for communications. The software is available for microcomputers operating under PC-DOS, MS-DOS, CP/M-80 and APPLE-DOS.

The system uses a proprietary algorithm. The alphanumeric key or pass phrase may be as long as 100 characters. The system does not store the key, so it is necessary to remember the key used for encryption. With this algorithm it is possible to repeatedly encrypt a previously encrypted file, and it is necessary to reverse the order of the process to restore the plain text.

Encrypted files can be stored locally or they can be sent through any electronic mail service, because all the encryption characters are printable ASCII; and because a carriage return/line feed has been inserted after every

65th character. Thus, files that could not previously be sent via electronic mail because they contained control characters, now are transmittable with P/C Privacy.

Another feature of P/C Privacy is that it allows users to do a screen comparison of the "checksum" for an original and decrypted file. A checksum is the sum of all the byte values in a file and thus it is like a fingerprint. If the checksums of an original and decrypted file do not match, then the user knows immediately that something has gone wrong in the transmission of a file, or the wrong key has been used to decrypt it.

In addition, this package has a purge feature that destroys all evidence of the original file before deletion. This is useful since files that are erased by removing them from a DOS directory may remain on disk and can be retrieved by using the Norton Utilities (a set of utilities which include programs to repair a damaged diskette, to recover erased files, to control hidden files, etc.). The purge feature actually over-writes the original file to zero and thereby eliminates any record of it on the disk.

3.2.2 DES-PAC (The trademark of Hawkeye Grafix Inc.)

This package is available for microcomputers operating under PC-DOS, MS-DOS and CP/M-80. It can

be used with any communications software which supports file transfer. Three basic operations can be performed by using functions available in DES-PAC such as , file encryption/decryption, compression/decompression, and SIXPAC formatting/deframming. These utilities are written in "C".

Encryption/decryption uses the DES algorithm. Three modes are provided which are Electronic code book, Cipher feedback and Cipher block chain. Each technique for encryption requires the user to input a 64-bit key or an eight character text string.

Compression/decompression allows a file to be reduced in size, the amount of which is dependent upon context. This reduction can range approximately from 10 to 50 percent, which greatly diminishes the transmission time and disk storage requirements.

SIXPAC formatting/deframming allows any file to be converted to/from a format similiar to a text file. The SIXPAC formatted file can be transmitted to any computer such as an information service box. A batch file is provided for ease of use in multiprocess operations such as compress, encryption, and SIXPAC.

3.2.3 DataSafe (The trademark of Trigram Systems)

This system is available for most of the CP/M, PC-

DOS, MS-DOS systems. It uses the NBS DES algorithm. Two modes are provided which are Electronic Code Book and Cipher Block Chain(CBC). Either mode can be set as the program default; CBC mode also allows the user to change the default initializing vector.

Two key schemes can be used. One can be an eight character hexadecimal key and the other can be an ASCII character string of at least eight characters. In either case, dual entry of the key is required for verification. The verification function determines whether the plain text has been encrypted and stored properly. It is not necessary to use it every time, but it can be helpful if the plain text is costly or impossible to recover.

The hexadecimal key function permits the user to generate a key randomly; this key method is more secure than an ASCII key. To use the key, however, the user must write it down, which can compromise the encoding unless caution is exercised to avoid destroying the written key, or permitting discovery of the key by another individual not authorized to know the key.

Two other useful functions are Checksum and Authentication. They provide the capability to detect whether a file has been changed either accidentally or by deliberate tampering.

3.2.4 PhasorCode 1000 (The trademark of Int'l Phasor Telecom)

This system, a menu-driven approach, is designed principally for microcomputers. It is available for PC-DOS/MS-DOS version 2. It secures confidential files in local computer storage and in file servers in local area networks.

It uses the RSA (Rivest-Shamir-Adleman) public-key encryption system. A public-key system uses different keys for encryption and decryption. That is, a public key to encrypt and a private key to decrypt. The system has automatic key management that provides for orderly control and use of both public and private keys. There is no limit to the number of encoding/decoding key pairs that can be created nor the number of public encoding keys the user may receive from potential recipients of secure messages.

Greater security protection is provided by using a pass phrase rather than a limited, single password. Any pass phrase from 8 to 32 characters may be used. In addition, it has following security enhancements:

- (1) Increased protection of encoded files and key directories. These files can not accidentally deleted by the DOS delete command.
- (2) Increased protection of decoding keys. To erase a decoding key, the user must first enter a secret

pass phrase to verify that he/she is authorized to erase it.

3.2.5 SECURE! (The trademark of Winterhalter Inc.)

The system uses the DES algorithm. It works with hard disk and floppy systems. It is available for MS-DOS/PC-DOS 2.X and 3.X compatible. The system is a combination of hardware(a PC bus board) and software.

It is an easy-to-use package. To encrypt a file or a directory, all the user has to do is to complete three simple steps. First, log in. Second, enter a password. Finally, choose the information to be protected. The system can show all directories and files in a graphic display form, easing file selection. To use encrypted files, the user simply logs in and runs his PC in the normal way. The system automatically decrypts the files when these files are used by the currently running program.

This system offers two levels of data protection to meet the user's security needs. It incorporates a master key feature designed for organizations requiring centralized administration. The security administration can gain access to all encrypted files and directories. Organizational information is given extra protection from employee loss, missing passwords, and other compromises in

security. For organizations not requiring centralized security administration, SECURE! allows individual users to immediately start using the system without the master key which lowers the organizations' administrative and installation expenses.

3.2.6 AutoCrypt I (The trademark of Jones Futurex Inc.)

This system provides transparent data security for the PC and XT computer systems. The system manager configures AutoCrypt I options according to the manager's requirements. The program then controls access to the system's files and programs by the user. This user transparent method of disk security encrypts all data as it is sent to the disk and decrypts it as it is read from the disk. Additionally, access control is provided through a user authentication code. This system is used with the Jones Futurex Encryptor 30X series of DES processors. Therefore, data going into the disk are encrypted under the DES algorithm.

With this system, a manager who has access to all machines assigns each user a key phrase up to 24 characters long. In conjunction with a master key which exists only in the data encryption processor. Only the manager's key phrase or a specific user's key phrase, identified by the encryptor board in the PC, can open up the data on a specific disk. Only the manager can make

plain text copies of the data, or allow another user to access it.

Chapter 4. Other Related Security Concerns

4.1 Risk Management

The most effective measure for protecting computerized data processing systems which handle sensitive information is through implementation of effective risk management procedures. Because each computer site and operating environment are unique, there are no standard solutions or checklists which can be applied to each site. Experience has shown that checklists tend to stifle development of effective and imaginative solutions to complex security problems.

The risk management methodology offers a disciplined approach through which undesirable events can be identified, measured, and controlled so as to minimize loss. Its application can, at the same time, assist in optimizing the amount of return from the security invested dollar. The cost potentials of broadly applied, marginally effective security features, are enormous and underlie the need for effective risk management at each site.

Two steps are needed for implementing an effective risk management procedure. The first step is to perform risk analysis and the second one is to perform risk assessment. Risk analysis has two main aspects [21]: 1)

identification of the undesirable events that can result, and 2) threat analysis. These undesirable events are usually categorized as follows: unauthorized disclosure, modification and destruction of data, and denial of service. Threat analysis also identifies the weak points in security that may permit each threat. Consider, for example, the threat that an unauthorized user may access the system from a remote site by means of a password found on a printout in the trash. Security weak points in this example are (1) inadequate physical security of the remote site; (2) failure to suppress printing of passwords; and (3) inadequate physical security of sensitive trash.

Once the risks have been analyzed, a risk assessment is carried out[21]. The undesirable events are rated and ranked according to severity. These ratings are not mathematically precise; rather they put risks into a priority order. The likelihood of each event is then related to its acceptability. A program for security is then developed, with the cost of each measure being considered in relation to the losses it is intended to prevent. All this information can then be used as the basis for a management decision about a security program. After such a program has been implemented, it must be monitored and evaluated periodically for effectiveness.

4.2 Personnel Security

Most computer - related crimes that have been uncovered were committed by company employees [15]. It would therefore seem logical that control should be exerted primarily over the employees using the system. Employee turnover or unhappiness is a major concern factor, and tends to occur when employees have low morale, or are emotionally upset, or are badly overworked. To minimize this likelihood, several practices can be adopted [21,23]:

- (1) High levels of performance and managerial abilities should be recognized.
- (2) Background checks on all prospective employees should be part of the standard operating procedures.
- (3) Ensuring that vacations are taken.
- (4) Employee cross-training will reduce the impact of turnover.
- (5) Providing grievance channels to allow employees to discuss sources of dissatisfaction without jeopardizing their positions.
- (6) Proper supervision should be provided for all employees. This will detect dangerous signals such as alcohol, gambling, etc., as early as possible.
- (7) Passwords should be disabled as soon as possible when computer-use authorization ends (that is, when a

user is fired, transferred, or resigned, or when a compromise is suspected).

Hemphill[7] suggests a self-assessment checklist for the management to determine if appropriate practices have been adopted to ensure personnel security. This checklist includes the following questions:

- Y N Does management realize there must be a basic reliance on the integrity of EDP employees and that this obviates the need for careful employee selection?
- Y N Is there a training program to make sure each employee understands his vital role in installation protection?
- Y N Does management insist on continuing with a problem employee?
- Y N Is management alert to changes in employees?
Is help extended to those who appear to be unstable?
- Y N Are employees required to leave the premises immediately if they are terminated?
- Y N Does management judge applicant stability by checking past residences, employments, and references?

- Y N Does management judge applicant stability by an examination of financial responsibility? By marital responsibility? By avoidance of arrest problems? By driving record?
- Y N When computer employees are hired in an emergency, are they on probation until all personnel inquiries are completed and evaluated?

If the management answers N to any of the above questions, this may indicate that the personnel security should be strengthened.

4.3 Contingency Planning

Computer centers often follow routines from day to day, intent on processing and current schedules, ignoring the problems that could arise during an emergency. But it is unrealistic to assume that the routine may continue indefinitely. Management must expect to be forced at some point to cope with the unexpected or the unknown. Practical planning, then, should take this into account.

One responsibility of computer security is to ensure that plans are made to backup critical hardware, software, and data; required emergency responses have been documented and roles assigned; and planning for recovery from disasters can achieve complete system operation in a

minimum time. Thus, in-place contingency plans are necessary to minimize the damage caused by unexpected and undesirable occurrences which might affect the system.

Donovan [3] mentions three general principles which underlies contingency planning: 1) The probability of occurrence of a disaster should be minimized - preventative measure; 2) The impact of a disaster, if it should occur, should be minimized; 3) The probability of recovering from a disaster should be maximized.

Applying these three general principles, it is possible to develop a well designed contingency plan. Such a plan would likewise consider the following three elements[10]:

- (1) Backup operations: Procedures to ensure that essential data processing tasks can be conducted after disruption of the primary facility.
- (2) Emergency response: Procedures to cover the appropriate response in such an event as fire, flood, water damage, bomb threat, or other natural disasters, to protect lives, limit damage, and minimize the impact upon the data processing operations.
- (3) Recovery actions: Procedures to facilitate the rapid restoration of data processing facilities following physical failure or destruction, or loss of data.

Chapter 5. Summary And Conclusions

This paper has presented four potential security problems that exist in the new data processing environment where microcomputers are used at end points. Several measures for solving the security problems in this new operating environment are described. These include:

- 1) Education programs for the first time end-user;
- 2) Measures for ensuring physical security of microcomputers;
- 3) Measures for ensuring logical security of microcomputers;
- 4) Measures for securing the telecommunication lines;
- 5) Application of the encryption technique for protecting data both in storage and in transit.

Last, three related security concerns for making the data processing environment including the microcomputers more secure were discussed. They are risk management, personnel security, and contingency planning.

End-user computing not only distributes processing, it also distributes the responsibility for security and control, and likewise distributes fraud and disaster if the organization is not careful. Even though there is no complete solution for all security problems, many measures will be present to ameliorate the severity of these security problems. Because of the microcomputer link, the corporate database has been exposed to a more hostile environment, since the central site has no control over

the data once it is sent out from the corporate database. As a consequence of this fact, the security of the mainframe may be weakened. To strengthen this environment, organizations should not only consider the security problems discussed earlier, but also must perform their own security assessment to determine the appropriate level of security that they actually need. In addition, strong support should come from senior management. If senior management believes that security is an important issue, then the security concern will not be relegated to a low priority. Finally, organizations should have their existing security system assessed periodically to see if their existing security program is appropriate to their current operational environment. Thus, as one can see, the future of end-user computing would be very bright if these security problems can be properly solved and controlled.

REFERENCES

1. Data Encryption Standards, FIPS publication 46, U.S. Dept. of Commerce/National Bureau of Standards, 1977.
2. Crocker, J. Micro/Mainframe links hold the key. DATA MANAGEMENT (January, 1984), 14-16.
3. Donovan, J. F. Industrial relations and contingency planning. COMPUTER SECURITY: A GLOBAL CHALLENGE, ELSEVIER SCIENCE PUBLISHING COMPANY, INC., New York, New York, 1984.
4. Falk, H. Microcomputer communications in business. Chilton Book Company, Radnor, Pennsylvania, 1984.
5. Goldstein, B. C. Directions in cooperative processing between workstations and hosts. IBM SYST J. 23, 3(May, 1984), 236-244.
6. Haneisen, W. D. and Camp, J. L. Business systems for microcomputer. Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1982.
7. Hemphill, J. M. Security Procedures for Computer Systems. Dow Jones-Irwin, Inc., 1973.
8. Highland, H. J. Impact of microcomputer on total computer security. Computers & Security, 1, 2(June, 1983), 171-183.

9. Highland, H. J. Microcomputer security: data protection techniques. Computers & Security, 1, 4(August, 1985), 123-134.
10. Highland, H. J. Protecting your microcomputer system. John Wiley & Sons, Inc., New York, New York, 1984.
11. Katzan, H. The standard data encryption algorithm. Petrocelli Books, Inc., New York, New York, 1977.
12. Lennon, R. E. Cryptographic architecture for information security. IBM SYST J. 17, 2(July, 1978), 138-149.
13. Lobel, J. The state-of-the-art in computer security. Computers & Security, 1, 2(May, 1983), 218-222.
14. Murray, W. H. Security considerations for personal computers. IBM SYST J. 23, 3(June, 1984), 297-303.
15. Norman, A. R. D. Computer Insecurity. Chapman and Hall, New York, New York, 1982.
16. Perry, W. E. The Micro-Mainframe Link. John Wiley & Sons, Inc., New York, New York, 1985.
17. Pollak, R. Micro-mainframe communications security in distributed networking environments. COM-SAC, 11, 2(September, 1984), A7-A15.
18. Prigge, E. Security and integrity issues of end-user computing. COM-SAC, 11, 2(September, 1984), A1-A5.

19. Pritchard, J. Data encryption. The National Computing Centre Limited, Manchester, U. K., 1980.
20. Schweitzer, J. A. Personal workstation automation security vulnerabilities. Computers & Security, 1, 3(March ,1984), 21-28.
21. Summers, R. C. An overview of computer security. IBM SYST J. 23, 4(December, 1984), 309-325.
22. Tanenbaum, A. S. Computer Networks. Prentice-Hall, Inc., Englewood Cliffs, NJ, 1981.
23. Ward, G. M. Securing a micro-mainframe link demands detailed action plans. DATA MANAGEMENT, December, 1984, 20-22.
24. Wood, C. C. Floppy diskettes security measures. Computers & Security, 1, 4(June, 1985), 223-226.

Appendix A. Trademarks

The following trademarks have been used in this paper:

<u>TRADE MARK</u>	<u>COMPANY</u>
AutoCrypt I	Jones Futurex Inc.
CP/M	Digital Research
CP/M-86	Digital Research
DataSafe	Trigram Systems
DES-PAC	Hawkeye Grafix Inc.
MS/DOS	Microsoft Corporation
P/C Privacy	MCTel
PhasorCode 1000	International Phasor Telecom Ltd.
SECURE!	Winterhalter Inc.
SIX-PAC	Hawkeye Grafix Inc.

Appendix B. Selected Sources Of Software

The following is a list of addresses for companies whose products are included in this paper. For product tradenames see APPENDIX A.

Hawkeye Grafix Inc.
3415 Hyde Park
Clearwater, FL 33519

International Phasor Telecom Ltd.
Suite 200, 1508 West 2nd Ave.
Vancouver, B. C.
V6J 1H2

Jones Futurex Inc.
3079 Kilgore Road
Rancho Cordova, CA 95670

MCTel
Three Bala Plaza East, Suite 505
Bala Cynwyd, PA 19004

Trigram Systems
3 Bayard Road #66
Pittsburgh, PA 15213

Winterhalter Inc.
3853 Research Park Drive
P.O. Box 2180
Ann Arbor, MI 48106

SECURITY OF MICRO-MAINFRAME LINKS

BY

Tzyy-Hsiung Chai

B.S., National Chung Hsing University, Taiwan, R.O.C., 1980

AN ABSTRACT OF A MASTER'S REPORT

Submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Computer Science

Kansas State University
Manhattan, Kansas

1987

ABSTRACT

The micro-mainframe link has greatly enhanced the concept of distributed computing. It improves the productivity of end-users on their day-to-day work and provides a wide variety of permutation and combination of activity. But at the same time, it increases potential security problems in the new data processing environment.

The majority of the newly introduced security problems are at the micro sites, since current operating systems for micros do not support the high-level security that is possible on mainframe computers.

In this paper, several measures for solving the security problems in the new environment are examined. In addition, other related security concerns which might strengthen the new environment are discussed.