ER 4320-87
16 September 1987

MEMORANDUM FOR: Information Systems Board

FROM: [redacted] STAT
Special Assistant to the Executive Director

SUBJECT: ISB Meeting Minutes - 15 September 1987

1. [redacted] STAT Computer Scientist for Engineering Group within OIT, discussed efforts to reduce the security risks posed by removable magnetic media through the use of "diskless" workstations. [redacted] STAT also conducted a demonstration of diskless workstation prototypes. A copy of the presentation slides is attached.

2. [redacted] STAT within IMS, described plans for a test-bed of diskless workstations in IMS. Notes from the presentation are attached.

[redacted] STAT

Attachments

THE "DISKLESS PC" CONCEPT: STRATEGY AND IMPLEMENTATION

Summary

This paper addresses the availability of methods for eliminating or reducing certain security problems associated with personal computers (PCs). Specifically, technology is discussed which eliminates the problems due to the storage media associated with PCs, but without the use of encryption. Encryption alternatives have not yet proven to be either effective or practical, and coverage of these problems and this technology is excluded from this discussion. The Director of Information Technology has specifically asked for solutions to the "floppy disk" problem other than encryption, and the scope of this paper is restricted to this issue rather than PC strategies in general.

The security problems introduced by storage media on PCs are many and serious. One solution is, however, conceptually simple--eliminate the media. The technologies and procedures to allow this are what need to be evidenced and are the subject of this document. A review of all the problems with storage media is not included, since it would be quite lengthy. However, a brief review of the types of media and the attributes of each is presented for background.

Background

The security problems under discussion are often characterized as "the floppy disk problem," but storage media on PCs actually takes several forms. One is internal "hard disk." This is obviously unacceptable for classified use in the absence of adequate physical personnel controls. But even in vaulted areas, hard disks still pose significant problems in aggregation of data, compartmentalized access controls between people in the vault, privacy, and information management concerns such as sharing, backup and maintenance. There are also removable hard disk drives which can be secured in a safe and which are designed for non-vaulted areas. Removable cartridge drives are the next form of removable "hard" storage and can be either magnetic or optical in nature. The removable media are followed downwards in scale by the familiar 5.25 inch floppy disks and the newer 3.5 inch units. This is actually just an ordered range of options for media, ranging from almost immovable to easily transportable. All suffer some security problems, trading some good points for other bad ones as the size and removability vary. The less transportable forms may have some valid utility in certain environments, but should never be assumed to be "secure" in the absence of strong procedural controls and correct data management practice. In any case, the most secure PC is one without any non-volatile media at all. Such a PC is generically called a "diskless PC."

[redacted] [redacted] 25X1

"Diskless PC" Technologies

Four technologies allow one to propose several varieties of diskless PC. Actually, the security goals do not require that the PC be truly without disks, merely that the disk either not be accessible or not permanent or not "writable." The use of volatile disk substitutes and "read-only" disk drives does not pose a hazard. Thus the four technologies are: disks simulated in volatile storage (RAM disk); disk services provided by a central, secure server (virtual disk); read-only disk drives; and networked disk services (LAN disk). These four concepts are not mutually exclusive, and actually are best used in combinations as circumstances require. Previous analyses of any one alternative at a time have generally missed the point that a combination is required to give adequate PC functionality.

RAM Disk

RAM disks are a standard commodity in the PC market, and are usually used to enhance performance of PCs without hard disks. Extra RAM (volatile random access memory) and software are installed to act as a high speed simulated disk, and sizes of 2 million bytes for a few hundred dollars are typical. The obvious security advantage is that the information on RAM disks can be almost instantly destroyed just with a program, or by turning off the power. Magnetic media cannot be sanitized by just overwriting it, but RAM memory can be. The obvious disadvantage is that information on RAM disk is lost if power to the PC is lost before the data can be transfered to a permanent storage medium on another, secure system. Certainly RAM disks could not be used in environments without stable power.

Virtual Disk

Virtual disks are simulated by host computer systems on behalf of PCs. The advantage is that the actual disk space is central on physically secured, backed-up, maintained systems with good access control facilities. This requires high speed connection between the PC and host, specifically "local" 3270 connections as can be provided usually only in a headquarters-like environment. Although there have been several implementations of this for IBM hosts and IBM compatible PCs, IBM's own strategic implementation (based on something called SRPI) will not be available until the later half of calendar 1987. Unfortunately, it may be available only for IBM brand software and perhaps even only IBM brand hardware until someone else clones this technology. Virtual disk usage requires very stable host systems as well, since the host going down is like a disk failure to the PC. For all these reasons, virtual disk technology is a potential candidate for some situations, but is not main stream as yet. However, one can still use host disk storage as a viable medium to assist in "diskless" PC use. High speed file transfer to and from the host can be used in lieu of true virtual disks. This is less "transparent" to the PC operator, but is commercially available from many vendors. File transfer is not very sensitive to host stability--as long as the host is generally available and not down for long periods. Also, there are other "micro-mainframe" link products that can be used on

"diskless" PCs for specific products on the host and which provide another tool for secure use of PCs.

Read-only Disk Drives

Read-only disk drives are a new concept which is not commercially recognized as yet, at least for magnetic media. Industry does provide the concept of read-only floppy disks, however, and this makes it trivially possible to extend the idea to read-only floppy disk drives. These are disk drives, specifically floppy disk drives, that will not write on disks but can still read them unimpaired. Low cost "after market" modifications to commercial floppy disk drives can produce such a read-only drive and change a PC with floppy disk drives into a read-only PC. This sort of PC has been dubbed a "neutered" PC to emphasize that it is not "diskless" but has been rendered non-threatening by surgery. This concept is not meant for hard disks, since such a modification would render them essentially useless. Read-only floppy disks are, by contrast, very useful in loading software into the PC. Since a PC floppy disk drive already has sensors and logic to detect and honor "read-only" disks (those with a write-protect "tab" on them), there is at least one trivial modification always possible to convince the disk drive that all disks are read-only and hence create a read-only drive. At least one company that performs "after market" modifications of PCs to satisfy peculiar customer requirements (e.g. TEMPEST) has already agreed to render read-only the PCs it sells if requested.

Read-only optical disk drives are also a potentially useful technology for more secure use of PCs. However, use of read-only optical disks (CDROM) is not a viable solution in itself, since no PC today can get started up ("booted") from optical disk. Also, the CDROM would only be a source for programs and reference material, not working files. Hence, the other technologies under discussion have to be used and the CDROM drive could only be viewed as an accessory. Other optical storage alternatives such as "write once, read many" (WORM) disks may also be useful adjunct to PCs if, for example, the disk is entirely pre-written with software before distribution and the disk drive is neutered just like a floppy disk drive. This would be a higher cost alternative that would provide more space but is essentially the same solution as for floppy disks in all other respects.

Networked Disk (LAN File Servers)

The last technology for removing the media from PCs is the use of networked files servers on local area networks (LANs). For PCs connected in a LAN, files can actually be made to reside not on each PC, but on a specific "file server" unit instead. This file server can be located remotely from the PCs in a physically secured area if desired and can enforce a reasonable degree of access control to the files it houses so that individuals at the PCs can only access files to which they have legitimate access. Different LAN implementations offer different mechanisms and degrees of control; but, at a minimum, password access to data is supported. The file server PC has to be maintained by a systems administrator for the group of people served by it.

Architecturally, this is exactly like a small departmental computer like a Wang Alliance, just implemented with PCs and a LAN. A LAN presents some unique security challenges in its own right, however. A complete discussion of a LAN architecture is beyond the scope of this discussion, but can be shown to be a viable technology with a great deal of value to the customers in its own right as well as a solution to the media security problem. No presumption of "secure" LANs needs to be made in order to implement them in a satisfactory way with commercial technology. The "diskless PC" problem with a LAN solution is that the each PC needs somehow to get started and hence generally has at least a floppy disk drive for booting even if connected to a LAN. Some vendors market truly diskless workstations, but this generally restricts the market to those vendors' LANs and devices and does not stay as strictly within the "IBM PC compatible" mainstream as one would like. However, this problem can now be solved in at least two ways. IBM and others will sell options for their local area network adapter cards which will allow a PC to "boot" from the LAN and never need disks at all. Or, one can use a combination technique and employ a PC with a read-only disk drive which would allow it to come up and get access to the LAN for all subsequent disk needs. This combination technique allows use of anybody's LAN and anybody's PC without constraints on competition. Admittedly, installing either IBM's network boot option or modifying disk drives to be read-only after purchase does make the PC somewhat custom and stretch the concept of staying in the commercial mainstream. However, addressing PC security cannot be done in the strictly commercial sense and these minor modifications of commercial PCs may actually represent the least "customized" solution. For specific applications where installing a local area network is not a problem, use of the commercially available diskless PCs (sometimes called "network terminals") might work fine without any customization.

Suggested Configurations

Clearly, stand-alone PCs with RAM disk or read-only disk make no sense--the range of solutions presented applies only to PCs as part of a larger information processing system or network. Depending on the network, there are two basic configurations that eliminate the media security problem.

Configuration 1

For a PC that is connected to a host via a high speed 3270 connection, a combination of RAM disk and read-only floppy disk drives is viable. The floppy disks are used for loading software only and are unclassified. Either one or two drives can be used, giving the customer access to up to 2.88 million bytes of programs without swapping disks if new IBM PS/2 technology is used (2.4 Mbyte if using older 5.25 inch floppies). By swapping disks, one can get by with only one drive and can still have access to unlimited amounts of software. To prevent accidental "fixing" of the disk drives to let them write, the read-only drives and the PC itself are visibly marked as being "read-only", and the PC case is key locked to prevent easy removal. (Some concern has been expressed about people "fixing" the PCs to write deliberately. The relevance of this

threat is for others to determine, but it would seem ineffective to go any farther in adding countermeasures since a truly hostile person who already has access to the classified data and who can smuggle electronic equipment in and out out the building probably is much more a threat in other ways than trying to fix floppy disk drives when more conventional tradecraft is safer and easier.) The PC itself and the program disks are all unclassified. RAM disk is used for all working files and to improve performance by copying frequently used software from floppy disk to RAM disk at start-up time. A RAM disk size of 2 Mbyte is recommended.

Configuration 2

The PC is the same as in configuration 1, but with the addition of a local area networking adapter, software and supporting network elements. The LAN adapter should have a network boot capability so that the PC can be started without any floppy disk in it at all. However, the presence of a read-only floppy disk drive is still recommended since it makes the network boot capability optional and provides a way to run software that is not available on the network for some reason. The presence of RAM disk in the PC is optional, but recommended for performance. The PC must be supported by a network file server with hard disks and a device for backups. Depending on the environment, this server might be kept locally in a customer's vaulted office area or in a separate vault for computers. Access to the file server would be limited procedurally and/or physically to a systems administrator. The backup device would be streaming tape or optical disk, media specific to this purpose and stored securely. This configuration would have no writable floppy disks anywhere on the network and would be equivalent in security to a Wang Alliance system. Host attachment is not required in this scenario, but can be provided if desired. Either each PC could attach individually just like the PCs in configuration 1, or the local area network could provide a "clustered" attachment point.

Operational Concepts

The "singleton" PC case, configuration 1, envisions a PC with host attachment only, no local area network. For a practical system, such a PC is really only useful as a very intelligent workstation for use with larger hosts. Such "PC terminals" can substantially improve customer interfaces, especially in word processing. Moreover, the hardware of configuration 1 is the right hardware to later add local area networks, optical disks, or whatever is required to build useful systems. The same device grows and can be used in many configurations and can be bought and used as a starting point well before all the questions surround LAN installations are resolved.

To use a "read-only" PC, the PC customer must be provided with floppy disks to start up the PC and supply those programs needed. These unclassified disks have to be created by the customer's application builders and modified to suit each individual's needs. An unclassified stand-alone PC either in the customer's office or an "Information Center" can be used to customize programs as desired. The procedural and support aspects of configuring software and

applications for read-only PCs are non-trivial since the individual user no longer does all the work himself to load and configure PC packages.

In use, the PCs would boot from the read-only floppy and an "automatic" procedure (AUTOEXEC.BAT) would create a RAM disk, copy performance-related files to it, set up the system so that working files would be put on the RAM disk, and start 3270 terminal emulation software and any applications software desired. The customer would then log on to the host if desired or work off-line at the PC, but the presumption is that the source materials are on the host and that the finished product returns there before the PC is turned off. Assuming that "virtual disk" support is not available commercially, use of the PC depends on file transfers between the host and PC. Application software can make the PC "front end" for the host with varying degrees of user friendliness, depending on the level of investment in programming.

A typical use would be by a customer using AIM and/or SAFE, where the primary interaction is with the host and the PC is used only transiently to prepare or edit files. These files are brought down to the PC for editing and shipped back up to the host for "filing." A number of procedures will be available to use PCs connected to the host in this way regardless of whether the PCs are "read-only" or not--this is just part of making PCs useful in conjunction with the host. Future development to provide a "windows" front end for an application like SAFE will work on a read-only PC just as on a "regular" PC. The only software that won't run on a read-only PC is something that is "copy protected" by a method that requires writing to the disk. However, this method of copy protection is all but extinct. Most corporate and government accounts refuse to buy copy protected software and hence almost no commercially successful software still uses any such scheme. The only real limits in the "read-only" PC approach are procedural difficulties for the customer. Files must be returned to the mainframe before powering off the PC. The host does not have to be "up" while the PC is in use, but must become available before the customer can finish the work. In environments where PCs are replacing terminals and offering new word processing power to be applied to files that are destined for the host anyway, a read-only PC is functional, though not as mistake-proof as a PC with disks.

In environments where there is only local processing (no host attachment) or substantial local processing, a local area network is required to make read-only PCs viable. For applications requiring extensive use of PCs for analysis, read-only PCs with only host attachment are not attractive, although they could be used in some cases with considerable loss in productivity. However, adding LAN functionality can not only ameliorate the ease-of-use difficulties, but add other new productivity aids and applications. As indicated, this sort of configuration is the logical equivalent of a Wang Alliance system, with the added benefit that each PC can also be host attached and hence have the best of both worlds--local processing and host processing. In a local area network, the PC has the equivalent of permanent local storage on the file server. Such a PC can be used exactly like one with a hard disk. There are really no functional issues in what the PC can or cannot do. There are some performance considerations in comparing network disks to internal hard disks, but the performance of the networked disk is generally sufficient to get the customer's job done. There are administrative issues associated with installing, main-

taining and operating the LAN in an acceptably secure manner. However, these issues have to do with the network itself, not the concept of "diskless" PCs. It is clear that in the long run, answering the dual questions of PC security and PC functionality will require LANs as part of the architecture.

Work in Progress

The use of "singleton" read-only PCs (configuration 1) has been explored within OIT. There appears to be no reason that the concept cannot be used to satisfy requirements for "terminals" for some components, specifically the DO. Work is required to use PCs at all as terminals, and this is progressing under the PCNEWS project umbrella. This work will apply equally well to a PC without writable disks as it does to any PC. As this PCNEWS software becomes available, it will be provided to customer offices to evaluate. Part of the evaluation for at least the DO will include use of "read-only" PCs to flush out any procedural and administrative issues. Clearly, providing "read-only" disks will place a greater responsibility on the applications developers and the "information centers" instead of the individual people sitting at the PCs, and each component will have to evaluate this.

Read-only PCs are also to be installed in a community environment for coordinating intelligence drafts. In this case, the "host" with the real disks will be just another PC. This particular project ("Coordinet") uses a "Windows" front end and the customers should not care that their PCs cannot actually write floppy disks.

Installing local areas networks of PCs has already begun in isolated instances, and activity to standardize and propagate such installations is underway. Installing only read-only PCs for all but the file servers is just a matter of deciding to implement the process of rendering disk drives read-only. OIT will install a testbed of certain LANs, including the IBM TRN to test out the "network boot" options available. However, commercially available diskless PCs already indicate that this is all functional and operable.

Internal Hard Disk Alternatives

A competing school of thought on PC security holds that internal hard disks are an acceptable risk in secure (vaulted) environments. This is basically a policy and regulatory issue. So long as the information on the PC hard disk is no more sensitive or compartmented than information that can be left on top of the customer's desks in a vault, most customers would not recognize the existence of a security problem. Actually, there are some issues such as aggregation of data and control and accounting for data files (Privacy Act, FOIA, document registry, etc.). However, these issues can be managed by education and policy rather than technology if desired.

Unfortunately, hard disks do pose some technical problems aside from the policy issues. Without floppy disks or some mechanism for backing up the data, the hard drives are too risky to use for important information. Thus a PC with hard disks and no floppy disk drive or a read-only floppy disk drive is

basically not feasible. Hence proposing PCs with hard disks as an alternative misses the target of eliminating floppy disks unless the PC is networked to a file server for backup anyway. And, if the PC is networked to a file server, the need for internal hard disks is reduced to a performance consideration only. Using host disks to backup the hard disk is also a possibility, but the performance and usability of the backup process to a host has yet to be demonstrated.

In spite of these reservations, PCs with hard disks are the commercial standard. It is becoming difficult to buy advanced PCs without hard disks, in fact. If their floppy disk drives are only used for backup and these backup diskettes are responsibly handled, PCs with hard disks can be lived with until local area networking becomes more widely available. For PCs not in vaults, removable hard disk drives are also something that should be considered as an acceptable interim solution to minimize or eliminate floppy disk use. Clearly, removable disk drives pose fewer risks than smaller, more easily concealed floppy disks. Configurations with a read-only floppy disk and two removable disk drives (for backup of each other) are not unreasonable.

Recommendations

1. OIT should continue efforts to refine and make available these diskless PC technologies. OIT must make available prototype models of read-only PCs for evaluation, and should ensure that consideration is given to the media security problems in all future supported configurations.

2. DO/IMS and OIT should jointly install a testbed of read-only PC terminals in order to expose all the technical problems, usability issues, and procedural requirements of such a solution to the DO terminal requirements. This effort must result in a finding as to whether this offers a solution to the 1988 and following year requirements for terminals, obviating the need to acquire (by trade) Delta Data terminals as soon as possible. OIT should also seek testbed opportunities with other Agency components to publicize the potential availability of these technologies.

3. OIT should conduct LAN testbeds with the objective of answering all relevant security issues and validating the concepts presented above for use of file servers in conjunction with read-only of diskless PCs. This testbed activity must coordinate with standards activities to define a supported configuration of read-only or diskless PCs and file servers. This effort must also address the various customer requirements for LANs.

4. OIT should coordinate all the interconnections of LANs among customer offices and from customer offices to remote locations such as a file server. A backbone grid of fiber optic cabling and distribution systems to support such a network is required and should be standardized upon and installed as rapidly as possible.

5. As soon as LAN standards and issues are agreed upon, OIT must undertake to select, install and maintain this technology. Furthermore, OIT should actively promote this technology and assist in defining solutions to cus-

tomer problems using diskless or read-only PC technology where applicable as part of any total solutions.

6. Existing policy publications on PC security are not effective in customer education, nor do they establish policy on information management issues. No policy on LANs is available at all. OS and OIT must prepare appropriate draft policy in all these areas, including a policy to minimize the use of floppy disks as much as possible. When coordinated and approved, these policies should become Agency regulations rather than mere guidelines and must be promoted effectively with education.

7. Interim use of internal hard disks in vaulted areas should be recognized as an existing fact and part of the price of participating in the PC revolution and staying within the commercial marketplace. The Agency must establish clear policy as to the role of internal hard disks, removable disk drives and how one should use floppy disks only as backup if at all. A choice must be made between living with the hard disks (internal or external) until some unspecified future technology is available, living with them forever, or proceeding at maximum pace to install networked (LAN) disks. If networked disks are installed, a commitment must be made to remove or render read-only the floppy disk drives and a decision must be made as to whether to keep the hard disks or use only the networked disks, trading performance for security.

8. OIT should continue to investigate optical disk technology to see if CDROM or other optical disk varieties can be used to make PCs more secure or more functional in secure configurations.