SYSTEM SECURITY?
As Soon As I Can Find The Time...

Steven G. Bloom
InCase Corporation
2055 Woodside Road, Suite 171
Redwood City, CA 94061

INTRODUCTION

Why is security so often talked about but just as often found at the bottom of the list of priorities? What we will be discussing will not be state of the art, brand new, never known before stuff about locking up the security on your HP 3000. You have probably read the many articles that have been written or will have heard the many talks given on how to close those nasty security holes. We will be reviewing some of these gems in this talk but my hope is that perhaps in understanding why security is so low on most of our lists, and realizing that it should be paid more than lip service, some system managers or MIS managers will return to their sites and take whatever action is necessary not next year, not even next month. Start reviewing your security procedures immediately! DON'T wait until your company becomes one of the fast increasing computer crime statistics! Although not nearly as fun as performance tuning, and certainly more likely to ruffle than smooth feathers, taking action NOW may save your company from a tremendous loss.

You might be surprised to discover how many system managers believe that they are safe from unauthorized intrusion even though they have taken no measures to protect their systems from unwanted access. Why do they believe that they are safe? Some state that their machines are only used by a very small group of people and that these people can be trusted with the data found on their HP 3000. Others say that this is merely a development machine and therefore, there is nothing to protect. Hmmm...

In this paper, we will be looking at the issue of security from the following perspectives:

- The history and growth of the HP 3000 business environment as it relates to security
- Specifics - What should be examined in the typical HP 3000 site?
- What is a security review? Who should perform it?

What are the measures being taken in HP 3000 shops today? In fact, they range from those mentioned previously, where even passwords are considered to be too much bother to the users, to shops in which only one user has access to an SM USER ID and every other user (with the exception of the single operator), logs into a tightly controlled, menu driven system with no access to the MPE colon (":") prompt. It is my perception that security concerns are of a lower priority in many HP 3000 shops than in facilities using other machines, such as DEC and IBM.

HISTORY

How did we get to our current state? To answer that question, we can look at the life cycle of the HP 3000 as a product line and its life cycle within a typical business environment.

Even in its early days, the HP 3000 was brought in to solve problems that were smaller in scale than those requiring the bigger "mainframe" computers. Then, as now, it was perceived as a "friendly" machine, not requiring an army of data processing professionals. An MIS department might only require an operator and perhaps a programmer. Due to its relatively low overhead requirements, the HP 3000 was (and is) seen as an excellent choice for a small company or division. These small companies often felt like "family" since everyone knew everyone else and everyone wore many different "hats". This contrasted to the big IBM shops where the complexity of the machine and of the operating systems required on-site system programmers and specialists in all aspects of system usage, including security.

ALL IN THE FAMILY

Many of those small companies that used the HP 3000 did not stay small. As the HP 3000 matured and grew more powerful, an increasing number of applications became available to the users. The users who once numbered in the tens were now pushing against the upper limit of an operating system that could handle 80 plus users at a time. Technical support staffs also grew and gradually, everyone no longer knew everyone else. The family had become a "community". However, as these small companies grew into bigger companies, no one wished to give up that feeling of "family", and so, there has been tremendous resistance to implementing policies and procedures that might have been considered as divisive or intrusive, such as security.

The resistance to implementing solid security was not only a result of the users' desire to maintain that warm fuzzy feeling of being part of a "family". In sites where "user ignorance" was the key to data security, even those technical support staff who agreed that the time had come for increased security measures responded with disdain at the notion that they should be locked out from total system access. I

have heard this from MIS managers who tell me that they are not concerned about improving security because the only ones with access to the MPE "colon" prompt are the programmers, and they, of course, must have access to all capabilities on the system. I wonder how many times a bug fix was overwritten by an enhancement or vice versa. I wonder too, how often this might have been prevented if carefully thought out change management policies and procedures had been implemented which could be enforced only by maintaining strict security on the system, including restricting programmers' access of a system.

The power of the HP 3000 has grown as well, and with that growth, there has been a parallel growth in the size of the installed base. Many of the early programmers and operators gained increasing knowledge of the operating system and its strengths and weaknesses. Some went on to create applications and utilities that would make the HP 3000 an even more attractive machine to solve a company's data processing needs. Some of these applications were sold and others were shared with other interested HP professionals at user group meetings. INTEREX formalized the software library and conference swap tapes. And of course conferences have permitted users to share knowledge through its speakers and through other contacts. Articles in trade magazines such as INTERACT have also played a major role in sharing the wealth of information and knowledge gained about MPE.

KNOWLEDGE AS A DOUBLE-EDGED SWORD

Unfortunately, the dissemination of knowledge that has occurred as a result of sharing information at user group meetings and through the contributed library has been a double-edged sword for security. Why? Because the CSL tapes and swap tapes are FILLED with privileged mode programs. Each one of these programs is a potential "trojan horse". Conference speakers on security love to talk about security holes in MPE and WELL THEY SHOULD! But again, knowledge can work for you or against you. While providing system managers with the information they could use to ensure a relatively secure system, the articles and talks also provide other technical people new ideas for hacking into a system that they can try out as soon as they get the chance.

The point here is that two parallel phenomena have occurred during the growth of the HP 3000 installed base. The first is that the interactive "friendliness" of MPE has helped to propagate the lack of concern for security in various ways. Although HP 3000 sites no longer are perceived as only being "small shops", we still like the warm fuzzy feeling that we are all "family" and so there is no reason to lock the door. Secondly, technical knowledge and understanding of MPE has exploded over the last fifteen years within the HP 3000 community as a whole, and has provided many the technical ability to break into minimally protected systems.

I JUST CALLED TO SAY "I LOVE YOU"

In addition to these two factors, another security-smashing monster looms high over our vulnerable data. DIAL-IN PORTS!! Communications from the field is no longer just "nice-to-have". For many companies, it is imperative that the field offices, sales people, service reps, etc. are able to access and update the necessary data in the system. Use of dial back modems is certainly to be encouraged but is not practical in many instances. How, for example, is the field representative going to be "dialed back" at a pay phone on Route 66 or at the customer's computer room? This means that unless an operator is standing by 24 hours a day, ready to UP or DOWN a dial-in port on request from the field, the system is vulnerable to anyone with a PC and a telephone. For all intents and purposes the system manager should treat the system as if it were attached to terminals at the local community college, which is virtually the case!

WHAT IS THE SOLUTION?

You aren't going to like the answer. There is almost nothing that can be done that will provide both an absolutely secure system, while at the same time allowing everyone, from programmers to users, the flexibility they all want. I believe that the answer is in INFORMATION. The system must be reviewed as a whole. Its strengths and weaknesses in terms of security must be weighed against ease of use and functionality as well as cost of change. You or your system manager must do a full security audit or review of not only the operating system security but of procedural and physical security as well.

Lets briefly review the three major areas of concern regarding security, physical, procedural, and logical.

Physical (or "Things that someone can do by wandering around")

- Is your CPU under lock and key?

  Access to the CPU or console is equivalent to access to your data for a knowledgeable intruder. If possible, the CPU, console, tape drive, and system printer should be in a room whose access is restricted to the minimum number of personnel.

- Is physical access to terminals restricted at all?

  Are any terminals in an area accessible to the general public? If there are, can this be changed? Can the ports to these terminals be DOWNed except when required?

- Are your modems accessible without either Dial-back or Operator control?

  The question to examine here is whether the outside world has access to your data? Are your modems physically accessible? Can an intruder simply "tap your line" at the modem itself? And most important, can a high school kid with a PC and a telephone get access to your data?

- Is access to the system printer restricted?

  Access to the system printer should be restricted, if possible. Valuable information should not be available to anyone with sticky fingers. Printouts should be kept in "lockboxes", available only to the user to whom they belong.

- How well is your tape and disc media protected?

  Tapes and disc packs kept onsite should be kept in a locked, fireproof room. Access to the key to the tape store room should be restricted to trusted individuals who have a bona fide need for access. Backup tapes should be stored offsite.

  Tape management is not just a disaster recovery issue. Accounting information is kept on a SYSDUMP tape which, if perused by someone who knows the tape layout, can provide useful information to an intruder.

- Is the console kept under absolute control?

  Don't distribute console capability lightly through the :ALLOW command. Again, be sure that there is a bona fide reason for granting special capability.

- Is a disaster recovery plan in effect?

  Although not a security issue, disaster recovery should be a major concern in any MIS organization that is charged with the management of critical corporate data. What would happen to your company if its general ledger, accounts receivable, engineering, inventory, sales, order management and manufacturing information bit the dust? There are disaster recovery plans available in many forms. If you do not yet have one in place, create one immediately!

Procedural (or "Things that someone can trick others into doing")

- Does anyone besides the OPERATOR have the ability to perform a STORE or RESTORE?

  This is a very important procedural question. Although MPE provides some safeguards on control of access to the tape drive through the REPLY required when a STORE or RESTORE is requested, this does not completely protect the system from an unscrupulous malefactor. A STORE tape could be given to the operator with instructions to REPLY to the tape request from what the intruder claims is a RESTORE that s/he has issued. In fact, the intruder has issued an FCOPY from the TAPE device which, once the unknowing operator has REPLYed to the request, will transmit all kinds of accounting information to a disc file that the intruder can examine at leisure.

- Are passwords required for all users on the system?

  Although there are usually accounts that contain little or no protectable files, remember that <u>any</u> access to the system might be dangerous. Once someone is logged on, the possibilities are much greater that illicit access will be acheived. Password <u>all users.</u>

- Are passwords required to meet minimum standards?

  Minimum Length. Passwords should be of a minimum length. I believe that a five character password is the minimum that forces a nontrivial effort to obtain the password through trial and error.

  No Jumbles. Passwords should NOT contain any combination of the characters in the USER ID, ACCOUNT name or GROUP name that it is protecting. (ie: SELBAYAP to protect PAYABLES)

  Change Default Passwords. Default passwords which are provided for third-party software accounting structures MUST NEVER be used.

  Not Easily Associated. Passwords should not be easily associated with the user to whom a USER ID is assigned. Spouse's or children's names may not be advisable in a user community where everyone knows everyone's family intimately. Second cousin's names are probably fine.

  Not Too Difficult. Passwords should not be so difficult for a user to remember that the password will have to be posted on the terminal. When possible, permit the user to change their own password or provide it to the system manager if no password changing program is available or desired.

- Are passwords changed on a regular basis?

  How often passwords need to be changed will depend on the specific requirements of your site. However, at the bare minimum, they should be changed at least every three months.

- Are individual users assigned unique USER IDs?

  Accountablility of action is impossible when generic USER IDs are used. There are a number of issues involved here. Firstly, individuals who are given their own unique USER ID are more prone to be protective of their passwords. If the user is informed that the password is his/her responsibility, and that activity performed by someone logged on with that USER ID will be attributed to the user to whom it is assigned, it is much more likely that the user will make a greater effort to protect the password and not give it out.

  Secondly, as I noted just now, with a unique USER ID assigned to each user, accountability IS possible. Reading the system log files will inform the system manager what system activities may have occurred at a given time by which sessions or jobs. But if the logon for a session was USER.PAYROLL, the manager will not be able to trace activity to a human being.

Logical (or "Things that someone can do from a keyboard")

- Are you using the default logon error messages?

  MPE, in all of its infinite friendliness, teaches a non-HP hacker everything s/he needs to know about breaking into the system. Each step of the logon process is clearly marked with what kind of information is required of the individual logging on. For example, typing garbage at the initial colon prompt results in CIERR 1402, which informs the hacker that the word required at this point is "...HELLO, :JOB, :DATA, OR (CMD) AS LOGON". The system will continue to aid the intruder as the breakin continues with useful information such as the eight character maximum length of a name.

  This problem does not exist on a UNIX logon. No matter what is entered, the user is not informed whether s/he has gotten into the system until both a logon id and password has been entered. And even then, the user is not informed WHY the logon failed.

Unfortunately for the security conscious among us, this is not the way things were designed in MPE. But you can at least reduce the helpfulness of the error messages in the message catalog, by changing ALL of the messages to one uniformly unfriendly message such as "LOGON FAILED". (Terry Simpkins wrote an article on just this topic in the October 1987 issue of INTERACT. It is worth reading.)

- Do you limit SM, PM and OP capabilities to the absolute minimum?

Without going into too much of the gory detail, I will explain briefly the danger in each:

SM: A USER ID with access to this capability can access any file with virtually no restriction. This means that the user logging on with this USER ID can purge, modify, execute, lock and append to any file on the system. That user can also change accounting structures virtually at will and can gain access to privileged mode (PM) which provides even greater ability to destroy, maim and mutilate.

PM: A USER ID with privileged mode capability has direct access both programmatically and through DEBUG to all machine instructions. A knowledgeable user with PM is, in fact, more powerful than a user with SM, because the PM user can actually bypass the operating system, whereas the SM user is still bound by the laws governing the operating system.

OP: Although a less dangerous capability, the System Supervisor, (OP), capability still should be of concern to the system manager. A user with OP capability has the power to STORE across account boundaries. Remember that the STORE tape can contain some interesting information to the potential intruder.

- Do you limit PM capability for groups?

A group with PM capability is dangerous even if the user with access to that group doesn't have PM. A PM program can only be run while it is residing in a PM group. Therefore, any PM program residing in a PM group could harm your data or even the operating system if run. But the scary thing here is that the user running the PM program doesn't have to have PM in order for the program to execute its privileged instructions! The answer then is to make sure that file access to the PM programs in the PM group are limited or that the PM programs that are accessible to all comers are "safe", right? Wrong! The PM group must be writeable only by trusted users in its entirety! Read on...

- Is your system safe from "Trojan Horses"?

  A non-PM user can create a PM program! To do this, the user must simply compile and link a program containing whatever nastiness s/he likes. Then the user need only patch the file to set the capability flag for the program to PM. Voila! A new PM program! This also implies that ANY program file to which non-trusted users have both write and execute access is dangerous. If I can write to it with FCOPY, I can inject my own super program into a mild mannered program residing in any PM group, even one in another account.

THE SECURITY AUDIT

The security audit is the system manager's way of judging the efficacy of the security procedures that have been put into place. The security audit or security review is really a checklist that can be gone through at regular intervals. The areas to be reviewed are the items mentioned earlier in this talk as well as other items that are of particular importance in your site.

Determining a security policy and creating a security review checklist occur simultaneously. Take the time to develop this policy now.

Who should perform this audit? In some locations, the audit is done by the system manager, while in others an outside auditor is brought in to perform this auditing function. There are benefits to both approaches which we will briefly examine here.

The external security auditor has some distinct advantages in terms of the objectivity that can be brought to bear in an individual site. It is sometimes difficult to see the forest for the trees when you are trying to delve into your own system. In addition, scheduling an external audit forces the job to get done, whereas it is easy to procrastinate and put it off when you are the one that must do the job. As the subtitle says, "As Soon As I Can Find The Time...".

On the other hand, the internal auditor has the experience and knowledge of a particular site. The internal auditor can develop a site specific security review that deals with the reality of that company's needs and corporate style. Often an external auditor will provide an audit checklist that is so standardized that it has no relevance to the needs of the client.

If you determine that an external auditor is the way to go, try to find a company or consultant that specializes in the HP 3000. Although security concerns are generic to some degree, there are things to watch out for that are system specific.