2

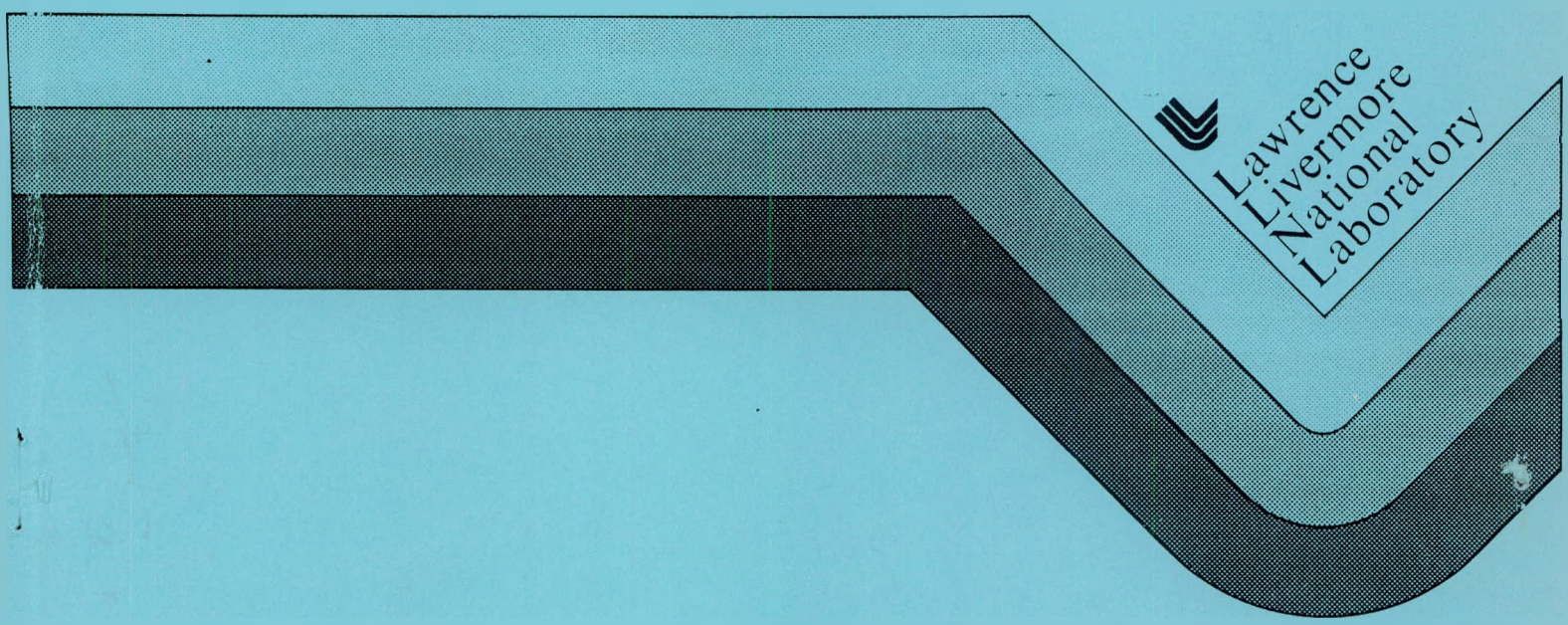
UCRL-MA-103440

SPI/UNIX User Manual
SECURITY PROFILE INSPECTOR

Version 1.2

Tim Tessin
Computer Communications and Security Group
Lawrence Livermore National Laboratory
P.O. Box 808, L-303
Livermore, CA 94550
(415) 423-4560

November 1989



DISCLAIMER

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

UCRL-MA--103440

DE90 011503

SPI/UNIX User Manual

SECURITY PROFILE INSPECTOR

Version 1.2

November 1989

DISCLAIMER

Tim Tessin
Computer Communications and Security Group
Lawrence Livermore National Laboratory
P.O. Box 808, L-303
Livermore, CA 94550
(415) 423-4560

Table of Contents

1. Introduction

The **Security Profile Inspector** (SPI) is a software security system for computers running the UNIX operating system. Its purpose is to assist system managers and computer security officers in providing and monitoring the security of a computer system. **SPI** inspects various aspects of the computer system and reports on inconsistencies or insecure features. **SPI** will also periodically check certain security features and will warn the system manager if any security policies are violated. Currently, **SPI** provides three major security inspections: the password inspector, the critical file integrity inspector, and the file permissions inspector. Future versions of **SPI** will include other areas of computer systems security.

SPI was designed to be very easy to use. All of **SPI's** major functions as well as other administrative functions are accessible through a **menu-driven** user interface. **Menu-driven** means that you can initiate computer security testing of a system simply by entering the number of one of the options displayed on the screen. You can set up the details of each test by entering values into easy-to-use forms. For more experienced users, all of SPI's functions are available as programs which may be run from the UNIX shell.

SPI will make your job of maintaining system security easier. However, it does not replace the system manager or computer security expert . Using a basic set of rules, **SPI** can check a system to determine potential security vulnerabilities. However, system managers and computer security experts must act upon the output which **SPI** produces to determine what changes in a system they should make to increase security. In the future, **SPI** might conceivably include some kind of elementary decision-making capability. Even with this capability, **SPI** will still only enhance people's ability to make decisions about computer security rather than to replace these people.

The **SPI** software can also be viewed as an on-line computer security training tool. **SPI's** user interface can provide on-line help information at any time. Future enhancements will allow the security officer to train new administrators with a tutorial session. *[Help is not available as of August 1989].*

This User Manual is divided into two primary sections. The first section explains each of the three main functions of SPI. The second section contains detailed instructions on how to actually run this software.

** Warning **

SPI contains programs and computer algorithms which are designed to find and analyze potential security flaws in computer systems. By their very nature, these programs and algorithms can be used by an intruder or inside violator to find and exploit the same security flaws. We recommend that the source code for compiling these programs be removed from the machine and kept protected from tampering and inspection. We also recommend that once the programs have been built, you make a copy of the executable files and keep them safe on removeable media, such as magnetic tape or floppy disk. If security was ever breached on your computer, you can use your backup copies to determine if your security programs have been tampered with. All possible precautions should be taken to prevent a non-trusted user from accessing SPI reports, parameter files and binary code.

2. What does SPI do?

The following sections provide an overview of what **SPI** does and the motivation behind its use. We recommend that you read the following sections at least once. A detailed description of the operation of **SPI** is found in section 3, **Using SPI.**

As its name implies, **SPI** inspects certain aspects of a system (such as the passwords for each account and the integrity of files) to determine how vulnerable that system is to intrusion. Each type of inspection is called a **function.** The types of functions available are described below. **SPI** functions are initially run to find security holes and to set-up a baseline (called a snapshot). It is then run periodically to monitor differences between the baseline and the current state of the system. Each section below will give guidelines on how to set up each function to monitor a system.

2.1 Password Inspector

The Password Inspector checks the password file for easily guessable passwords. (In UNIX, the password file can usually be found in **/etc/passwd** .) The password file contains information such as account names, passwords, project names, and a comment field (GCOS field) that usually contains information about the user. **SPI** checks passwords in the password file against various dictionaries and certain algorithmic permutations to find passwords which are easy to guess or find using trial-and-error methods. The system manager can choose which dictionaries and permutations to use. The checks include the following:

- Comparing 1, 2 or 3 letter combinations of alphabetic or numeric permutations against users' passwords to determine if any match.
- Comparing users' passwords against passwords derived from the GCOS field of the password file.
- Comparing users' passwords with entries in three separate dictionaries: common English words, local jargon, and trivial words (e.g. names of characters is books or names of cars).

Additionally, the Password Inspector checks for accounts without a password, or has a password which is too old. Old passwords could indicate an inactive account. Passwords should be changed at regular intervals to prevent a compromised password from giving unlimited access. **SPI** has a mechanism for finding old passwords. It involves initial setup of a log file and subsequent checks using this log file. For more information on setting up and using a password log file refer to sections 3.3.1.3 and 3.3.1.5.

As you configure the Password Inspector function, you will be able to choose the type of tests you want to perform. We recommend that you use the default dictionaries provided by **SPI.** We also recommend that you customize the dictionary called **local.pass** to reflect local jargon used at your site since passwords consisting of local jargon are extremely vulnerable to compromise. For information on how to edit a dictionary refer to section 3.3.1.6

The **SPI** Password Inspector uses the Unix library function *crypt(3)* to check passwords. The crypt function was designed intentionally to be slow to prevent "brute-force" cracking attempts. A typical UNIX machine can try anywhere from 2 to 10 attempts per second. This means that trying 25 password entries using approximately 30,000 words (dictionary plus trivial passwords) will take on the order of 40 hours of CPU time. Additionally, checking all permutations of 3 characters will almost double the run time. We recommend that you only run a full check once when you first install **SPI**. Because the Password Inspector uses a password log file, **SPI** will only check the passwords which have changed since the previous check. The Password Inspector should be run at least once a week to check any passwords changed during the week. For users with more stringent requirements, we have a special version of the *crypt(3)* function which speeds up password checking by a factor of 30-40. Contact the **SPI** development team in the Computer and Communications Security Group at Lawrence Livermore National Laboratory for further details. The team can be reached by electronic mail at *ccsg@tiger.llnl.gov*.

2.2 File Integrity Inspector

The File Integrity Inspector checks if a set of files have been modified with respect to a given baseline. It compares the **crypto-checksum** of a file against a known checksum obtained from the initial run (snapshot) of the File Integrity Inspector. A **crypto-checksum** is a numeric value generated by a mathematical algorithm that uniquely identifies the contents of a file. This method is better than checking the last time a file was modified, since a knowledgeable intruder can reset the time of last modification to hide the changes made. If the current checksum is different from the previously stored value, the file has been changed since the last check. The File Integrity Inspector's primary use is to detect whether or not a set of files critical to the operation of the system have been altered; although the system manager can designate any set of files (critical or not) to be checked.

During **SPI's** installation procedure, a list of "critical files" is created by searching the contents of a few important system directories (e.g.; /bin, /usr/bin, /etc). The list should be examined to make sure that all the important system files are present as well as any other files you wish to be checked. **SPI's** user interface provides for list maintenance. You can edit any File Integrity Inspector list by selecting the "edit" option on the File Integrity Inspector form. For further information on list maintenance refer to section 3.3.2. You can keep several sets of file lists. As soon as these lists are complete, you should "snapshot" the lists by selecting that function from the form. This will create the baseline for further checks. Note that the File Integrity Inspector is **SLOW** and the screen will not change until the snapshot has completed. This can take a long time. Most critical file lists will take a couple of hours to check. The crypto-checksum program can calculate at the rate of 2K bytes per second. This will be fixed in a later release.

Depending on how many files are in the list, you can run the File Integrity Inspector each evening. This will give you an indication of what files have changed during the day. Files like the *password* file will change fairly often, but knowing that the file has changed will help the system administrator determine if the changes are routine or malicious.

2.3 Critical File Permission Inspector

The Critical File Permission Inspector checks and compares the permissions on certain files with the recommended (or user-supplied) permissions. The permissions on a file determine who can do various things with the file, such as reading, writing, or executing the file. If system critical files have improper permissions, an intruder or careless user could overwrite or otherwise tamper with them. This function reports any differences in permissions from what the system manager has determined they should be. When **SPI** is installed it creates a list of "critical files" by searching the contents of a few important system directories (e.g.; /bin, /usr/bin, /etc). This list should be examined to make sure that all the important system files are present.

SPI's user interface provides the same type of file maintenance for the File Permission Inspector as that for the File Integrity Inspector. You can edit any File Permission Inspector's file list by selecting the "edit" option on the File Permission Inspector form. You can also keep several sets of critical file lists. As soon as these lists are complete, you should "snapshot" the lists by selecting that function from the form. This will create the baseline for further checks. Once the snapshot is complete, you should examine the "snapshot" file to make sure that the permissions are correct for your system. For more information concerning "snapshot" files refer to section 3.3.3. Ideally, none of the system critical files should be writable by anyone other than system accounts. A default list of recommended permissions is not provided due to the many variations of Unix systems, but you can contact the system vendor or the Computer Incident Advisory Capability (CIAC) team at Lawrence Livermore National Laboratory for hints and possible recommendations. The CIAC team can be reached via electronic mail at *ciac@tiger.llnl.gov*.

Unlike the File Integrity Inspector, the File Permission Inspector is fairly quick and, therefore, should be run nightly. This will give you an indication whether any critical files' permissions have been changed.

3. Using SPI

The instructions in this manual are based on the assumption that you are using a VT100 terminal, or are running a VT100 emulation package. **SPI** can be used with any terminal which has a correctly functioning "reverse video" and is correctly described in the UNIX *termcap* or *terminfo* database. We suggest that you briefly read over sections 3.1 through 3.4 once to get an overview. Then go over each section in detail while actually running **SPI.**

3.1 Starting SPI

There are two ways to start **SPI.** One is by using menus and is explained starting with Section 3.2. The other is by using the UNIX shell and is explained in Section 3.4. **SPI** has no special permissions, so in order for it to access the entire system, you must be logged in under the **root account** or running as **superuser.** To start **SPI's** user interface type:

```
spi <return>
```

This will execute the **SPI** menu session. If **SPI** is not found when you try to run it, check to see if you are in the **SPI** installation directory. If you wish, you may put the **SPI** installation directory pathname in your shell path variable. For more information on UNIX shell pathnames refer to the UNIX documentation for your system concerning the shell you are using. If you do not want **SPI's** path in your shell path variable, be sure to enter the entire path name to **SPI** or start **SPI** from its installation directory.

3.2 Using SPI Menus

Once you have started the **SPI** program, the main menu will be displayed. The main menu should look like this:

```
S E C U R I T Y   P R O F I L E   I N S P E C T O R

    1  Select Password Inspector Parameters
    2  Run Password Inspector
    3  Select File Integrity Inspector Parameters
    4  Run File Integrity Inspector
    5  Select Critical File Permission Inspector
    6  Run Critical File Permission Inspector
    7  Select Run Time
    8  Display Output
    9  Quit

    Enter selection number:  __

Previous Page <cntl p> Next Page <cntl n> Previous Field <cntl b>
Return to Menu <esc> Help <?>
```

Figure 1

SPI Main Menu

If the main menu on your screen does not look like **Figure 1**, exit **SPI** by selecting 9 and press the <return> key or the <escape> key. Then check your environment to be sure that the environment variable, TERM is set correctly. You may also want to ask the system manger to check the */etc/termcap* entry for your terminal.

There are nine menu options representing the nine functions available. Some of these selections (1,3,5,7) are *configuration* options. These options enable you to configure the way in which **SPI** will run. You can, for example, select which files **SPI** will read, the nature of password tests, the exact time(s) at which **SPI** will run, etc. Other options (2,4,6) are *run* options, each causes an inspector (Password Inspector, File Integrity Inspector, or Critical File Permission Inspector) to run immediately. For example, if you choose the Run Critical File Permission Inspector option, the Critical File Permission Inspector will run without any further delay. The rest of the options are auxiliary functions. For example, option 8 lets you select which report to view.

To select a function, type the number for that function (from 1 to 9) and press <return>. You must press a number key from the keyboard. For options 1, 3, 5, 7 and 8, once you have entered the number and pressed the <return> key, the menu will be cleared from the display screen, and a form belonging to the function you have chosen will be displayed. If you enter options 2, 4 or 6 and press the <return> key, the main menu will flash signifying the acceptance of your choice. You will be notified by electronic mail which is mailed to the account you specified during installation when your selection has completed. If you type the wrong number (e.g., 12) and catch your mistake before you press <return>, you can rub out this number. If you type the wrong number and then press <return>, a message, displayed in the error field at the bottom of the menu, accompanied by a beep will inform you that you must enter a number between 1 and 9. The error message waits for you to acknowledge that you have read it by asking you to press the <return> key. The menu will remain on the display screen until you select one of the functions.

When you are through using **SPI**, press the <escape> key or select option 9, then press the <return> key. **SPI** will terminate and return to the UNIX shell prompt.

3.3 Using SPI Forms

If you have chosen a *configuration* option, the next thing you will see is a form. Filling out a form is a convenient way to supply information to **SPI**. A form consists of the name of the function at the top followed by a set of fields. Each field has a descriptive message to the left of the input area which describes the data to be entered. At the bottom of the form are two special fields used by **SPI** to convey prompt and error messages to you. The input area is defined by the area to the right of the explanation on the same line whose background is the opposite of the rest of the form (reverse video). Its length represents the maximum number of characters allowed in that field.

To fill out a form, type the desired information into the current field (where the cursor starts), then press <return>. Once you enter information into a field and press <return>, the cursor will automatically move to the next field in most cases. If you type more characters then the maximum allowed in a field, the last character will be overwritten by the characters you are typing. If you need to back up and correct errors in your field entry, type a <backspace> and the current character will be erased.

Some forms have fields which are called dependent fields. They are set off from other fields by indentation from the field they depend on. A field followed by a dependent field may look like this:

```
Use Local Password Dictionary?  (Y/N):
   Local Password Dictionary Filename:
Use Standard Trivial Password Dictionary? (Y/N):
```

The user is asked to fill in the dependent field depending on the answer to the field depended on. In the example above the question, Local Password Dictionary Filename depends on Use Local Password Dictionary. In this example, a "Y" answer will cause **SPI's** user interface to ask you for the Local Password Dictionary Filename, a "N" answer will cause **SPI's** user interface to skip to the next question, Use Standard Trivial Password Dictionary. In any field except the error message field, if you want the cursor to move back to the previous field, press <control> and the 'b' keys simultaneously. This and other information discussed later can be found at the bottom of the form in the prompt fields.

If you make a mistake while entering information into a field, you can rub out one letter/number each time you press <backspace>. If you entered incorrect information into a field and pressed <return>, you need to move the cursor back to that field and correct the mistake by entering the correct information and pressing <return>. (Note that <backspace> is really a *delete* function and *not* a means of moving the cursor to a previous field as mentioned above by pressing <control> b, which will move the cursor to the previous field.)

Some explanations which precede a field show information in parentheses. For example, you might see:

```
Use Previous Password Log File Name? (Y/N):
```

The information in parentheses tells you what you can enter into the field. In the above example, you should type either Y (for yes) or N (for no), then press <return>. If you enter anything other than Y or N, an error message will be displayed.

In some cases, a **default entry** will be displayed in a field. The default entry is a value determined to be one that most users require. Initially **SPI** uses the defaults in the distributed default configuration files. These values should by modified to meet your needs and saved in a new appropriately named configuration file. Once you have used **SPI**, the default file (whose contents will be displayed in a form's fields) will normally be the last configuration file you created for that form. If at any time you want to use the distributed default configuration file, you can by selecting the appropriate default file name for the inspector you are configuring. The following is a list of the Inspectors and their default files.

Password Inspector	**default**
File Integrity Inspector	**master.list**
Critical File Permission Inspector	**master.list**

For further details refer to the sections concerned with configuration files and file name lists for each inspector.

If you prefer the default value for a field, simply press <return> when the cursor is in that field. The default value will be accepted by **SPI**. You may also type over any default

values with a new entry. If you type a character or a number while the cursor is at the left of a field which has a default entry, **SPI** will automatically clear the rest of the default entry for you.

When you are through filling out the **Password Inspector** forms or the **Run Times Schedule** form, **SPI** will ask you if you want to save the information you have entered. The last field on these forms is:

```
Save All Choices You Have Made for this Form? (Y/N):   Y
```

The default entry for this field on the **Password Inspector** is N (no). The default entry for this field on the **Run Times Schedule** form is Y (yes). If you enter Y, **SPI** will save all the entries you have made in a new file. **SPI** will ask you for the new file name. All of the values you have previously entered will be saved in that file and that file will be used for the default values the next time you use that function. This will allow you to have different configurations without having to reenter the data.

To exit from any form, simply press the <escape> key. The form with which you have been working will be cleared from the display screen, and the menu will appear again. If you need help, simply press the ? key. *[Help is not available as of August 1989].*

3.3.1 Password Inspector Form

Since this form is the only multi-page form in **SPI**, it is time to introduce a few more form manipulation characters. **SPI's** User Interface has two specific form manipulation control characters. These are the <control> p, and the <control> n keys. At any time while a form is displayed on your screen you can display the next page of the form by pressing the <control> and 'n' keys simultaneously (note: the cursor will be positioned in the first field). The <control> and 'p' keys will display the previous page of the form (note: the cursor will be positioned in the last field of the form). In either case data is not lost except for the situation noted below under caution. In addition to these characters, pressing the <return> key at the bottom of a form will display the next page of the form and pressing the <control> b keys at the top of a form will display the previous page of the form. In the case of a single page form the form manipulation characters do nothing. Pressing the <return> key at the end of a single page form will position the cursor in the top field of the form. Conversely the <control> b keys simultaneously pressed while at the top of a single page form will position the cursor in the bottom filed of the form.

**** Caution ****

*Entering a <return> causes the data in a field to be accepted. If you type <control> N or <control> P **before** you hit the return key, any changes to the current field entry will **not** be accepted. You will not know this unless you page forward or backward to recheck your entry. Make sure you type the <return> key before paging forward or backward.*

```
                    P A S S W O R D   I N S P E C T O R      Page 1 of 3

   SET-UP
      Password Inspector Parameter File to Read: default
      System Password Filename:                  /etc/passwd
      Create New Password Log File? (Y/N):       Y
      Starting Account Name:                     ________
      Ending Account Name:                       ________

   PREVIOUS PASSWORD LOG FILE
      Use Previous Password Log File? (Y/N):     Y
          Previous Password Log Filename:        psi0801289
          Check for Old Passwords? (Y/N):        Y
             Maximum Age (###)days(s):           180


Previous Page <cntl p> Next Page <cntl n> Previous Field <cntl b>
Return to Menu <esc> Help <?>
```

Figure 2

Page 1 of the Password Inspector Form

You should fill in the fields of the Password Inspector form as follows:

3.3.1.1 Password Inspector Parameter File to Read:

The data in the configuration file you choose will be used to set the default values for the rest of the fields in this form. The configuration file name you enter here should be one that you created during a previous session (refer to sections 3.3.1.16 and 3.3.1.17) or the distributed default file. The distributed configuration file name is "default". If you enter a file name that does not exist, **SPI** will tell you with a message in the error field. Unfortunately, at this time, **SPI's** User Interface can not display all the possible configuration file names. These files are located in the **SPI** sub-directory *parameters/psi* and can be listed using the UNIX "ls" command (the filename "psi" is special and should not be used). Your entry into this field can be up to a maximum length of 21 characters.

3.3.1.2 System Password Filename:

NOTE: This option only works on UNIX systems that support more then one password file. It also does not work for those systems that have password shadowing. Check with your system manager before changing the default value of this field.

This entry determines which password file will be inspected. You can enter any path and filename, but the maximum length of an entry is 21 characters. **SPI's** User Interface will check for the existence of the file you enter and inform you if it does not exist. The initial default filename is **/etc/passwd.** Please note that if you do not accept the default file, /etc/passwd, the file you use must have the same record format layout as /etc/passwd. In other words, the file you use must look like a password file. (For more information about record format layouts, consult a UNIX reference manual, or see your system manager.)

3.3.1.3 Create New Password Log File? (Y/N):

This entry (Y or N) determines whether **SPI** will create a password log file when the Password Inspector, option one of the menu, is run. If you wish to check for expired passwords in future runs of the Password Inspector, you must create a password log file. Currently log files are automatically given a name that starts with **psi** followed by the current date of the run. For example, a log file created during a run on February 14, 1988 would have the name psi021488. Unfortunately, a subsequent log file created on the same day will over write the first log file. At this time, **SPI's** User Interface does not provide a means to list all the log file names. They can be listed using the UNIX "ls" command in the **SPI** sub-directory *parameters/psi*. The first time you use the Password Inspector, the default entry will be Y (yes). Afterwards, the default value will be whatever value specified in the parameter file you choose in section 3.3.1.1.

3.3.1.4 Starting Account Name:

This entry (maximum length: 8 characters) determines the account in the password file from which the password comparison tests will begin. If you do not know the account names, view the password file. The account names are in the first field of password file record.

This an example of the contents of a password file entry:

account name	Encrypted Password	User ID	Group ID	GCOS Field	Home Directory	Startup Shell
abrahams	x4D.P#sR	666	777	Seth Abrahams, CCSG, LLNL	/users/abrahams	/bin/sh

If you do not wish to designate an account name from which the password comparison tests will begin, you can simply press <return>. A blank account name in this field tells the Password Inspector to examine the entire file. Since you did not designate a starting account SPI's User Interface will not ask you for an ending account. The cursor will advance to the **Use Previous Password Log File** field.

Ending Account Name:

This entry determines the account in the password file on which the password comparison tests will end. Your system manager can inform you of account names. The maximum length of the ending account name is 8 characters.

3.3.1.5 Use Previous Password Log File? (Y/N):

The first time you use the Password Inspector, or if a password file has not been created, you need to enter N into this field. Once you have created a password log file (refer to section 3.3.1.3) you can use that file to check for new passwords and those that are older then a specified number of days. If you enter N, the Password Inspector will not use a previous password log file for comparisons, and the cursor will move to the **Use Local Password Dictionary** field at the beginning of the next page.

Previous Password Log File Name:

If you chose to use a previous password log file, the Password Inspector must know the name of the log file you wish to use (maximum length: 21 characters). The default previous password log file name is the name found in the password inspector parameter file designated in the first field of this form. You may, however, wish to enter the name of another log file. For example, if the day you made the log file was April 5, 1989, you should enter **psi040589**. Once again SPI's User Interface does not provide a means to list all the password log files. You can list these files using the UNIX "ls" command in the **SPI** sub-directory, *parameters/psi*

Check for Old Passwords? (Y/N):

If you accept the initial default value, Y, the password file you have specified previously will also be checked for passwords which have not been changed for a certain number of days. If you enter N, the password file will not be checked for old passwords, and the cursor will move to the **Use Local Password Dictionary** field at the beginning of the next page.

Maximum Age (### days):

If you elected to check for old passwords, you need to specify how old the passwords can be. You can enter up to a maximum of three digits into this field. The initial default value for this field is 0. (If you choose the default value SPI will consider every password to be "old," and will check every one.) If you enter 7, the password inspector will check passwords which are older than seven days. If any passwords are found to be older than the number of days you specified, the password inspector will report the old password and the last date it was modified.

After you make an entry in this field, the cursor will move to the *first field on the second page of the form.*

```
                    P A S S W O R D   I N S P E C T O R          Page 2 of 3

   DICTIONARY CHECKS
      Use Local Password Dictionary? (Y/N):                  Y
         Local Password Dictionary Filename:                 local.pass
      Use Standard Trivial Password Dictionary? (Y/N): Y
         Trivial Password Dictionary Filename:               trivial.pass
      Use Full Password Dictionary? (Y/N):                   Y
         Full Password Dictionary Filename:                  /usr/dict/words

   SECURITY CHECKS
      Try Alphanumeric Permutations? (Y/N):                            Y
         Maximum Permutation Length (1/2/3):                           3
         Try Upper-Case Permutations? (Y/N):                           Y
      Try Reversed Dictionary Passwords, Login Names, etc.? (Y/N): Y
      Try Passwords Converted to Upper-Case? (Y/N):                    Y


Previous Page <cntl p> Next Page <cntl n> Previous Field <cntl b>
Return to Menu <esc> Help <?>
```

Figure 3

Page 2 of the Password Inspector Form

3.3.1.6 Use Local Password Dictionary? (Y/N):

This entry determines if the password file will be tested against a list of local passwords, i.e., passwords which are frequently used at a particular site. If you enter N, the cursor will move to the **Use Standard Trivial Password Dictionary** field.

Local Password Dictionary:

If you have chosen to use a local password dictionary, you must specify the filename of that dictionary. The maximum length of this filename is 21 characters. The first time you use the Password Inspector, the default filename will be **local.pass**. In later uses, the default will be what ever is specified in the Password Inspector's parameter file (section 3.3.1.1). **Local.pass** is a dictionary supplied in the distribution and is located in the **SPI** sub-directory *parameters/psi*. If you want to specify your own dictionary, either move it into the *parameters/psi* directory or specify the entire path name to the dictionary file. If you can not move the dictionary and the path name is to long for the field, you can create a soft link in the *parameters/psi* directory to your dictionary and use the name of the soft link. For more information on soft links refer to the UNIX "ln" command in your UNIX section 1 manual. If you enter a dictionary name that **SPI** can not find, **SPI** will issue an error message.

We recommend that you copy the **local.pass** dictionary and edit the copy to include passwords reflecting local jargon of your work environment. The **local.pass** dictionary file is located in the **SPI** sub-directory *parameters/psi* . You should use the name of the new dictionary in this field.

3.3.1.7 Use Standard Trivial Password Dictionary? (Y/N):

If you enter Y, the password file will be checked against a list of passwords which we have found to be highly guessable (e.g., wizard, manager, proper names). The cursor will then move to the field immediately below this one. If you enter N, the standard trivial password dictionary will not be used to check the password file, and the cursor will move to **Use Full Password Dictionary.** The initial default for this field is Y.

Standard Trivial Password Dictionary Filename:

The manipulation of this field is the same as that for the **Local Password Dictionary** field. The default filename for this field the first time you use the Password Inspector is **trivial.pass.** This dictionary also resides in the **SPI** sub-directory *parameters/psi.*

3.3.1.8 Use Full Password Dictionary? (Y/N):

This entry determines if the password file will be checked against a list of English words. This check will be performed if you enter Y. The cursor will advance to the next field, **Full Dictionary Filename.** If you enter N, the full English dictionary will not be used to check passwords. The cursor will then move to the **Try Alphabetic Permutations** field in the next section of this form. The initial default entry is Y.

Full Dictionary Filename:

The initial default English dictionary filename is the UNIX dictionary which usually resides in **/usr/dict/words.** If your system does not have **/usr/dict/words** an alternate dictionary is provided for you called **dict.words.** The manipulation of this field is the same as that for the **Local Password Dictionary** field. After you make an entry into this field (maximum length: 21 characters), the cursor will move down three lines to the **Try Alphanumeric Permutations** field in the next section of this page.

3.3.1.9 Try Alphanumeric Permutations? (Y/N)

If you enter a Y into this field, **SPI** will automatically create permutations to use as guesses for passwords. After you designate the maximum permutation length and whether you want to include upper-case permutations (in the next two fields), **SPI** will attempt to match the passwords against the list of permutations it has created. If you enter N, **SPI** skips checking alphanumeric permutations, and the cursor will move to the **Try Reverse Passwords, Login Names, etc.** field. The initial default value for this field is Y.

Maximum Permutation Length (1/2/3):

If you elect to try alphanumeric permutations, you need to specify how long you want these permutations to be. You may choose lengths of 1, 2 or 3. The initial default value is 3.

Try Upper-Case Permutations? (Y/N):

You need to specify whether you wish to use upper-case permutations in matching alphanumeric permutations against the password file. The initial default value is Y. If you choose this value, **SPI** will add the tests for upper-case alphanumeric permutations to the others you have selected. This will double the time for SPI to run the permutation tests.

3.3.1.10 Try Reversed Dictionary Passwords, Login Names, etc.? (Y/N):

This field is another field in which you must make a yes-or-no choice. If you enter Y, **SPI** will reverse the order of the strings in all the tests you have selected above and double the number of strings to use to guess passwords. If you enter N, **SPI** will not create reversed string orders. The initial default value for this field is Y.

3.3.1.11 Try Passwords Converted to Upper-Case? (Y/N):

If you enter Y, **SPI** will perform an additional matching test with all the strings you have selected above converted to upper-case, thereby, doubling the number of strings used to guess passwords. If you do not want to include upper-case password guesses in the password tests, enter N. The initial default value is Y.

After you make an entry in this field, the cursor will move to the *first field of the next page of this form.*

```
                    P A S S W O R D   I N S P E C T O R          Page 3 of 3

  REPORTING OPTIONS
    List All Account Names Tested? (Y/N):                  Y
    List Changed Accounts? (Y/N):                          Y
    List New Accounts? (Y/N):                              Y
    List Passwords When Matched? (Y/N):                    Y

    Save All Choices You Have Made for This Form? (Y/N): N
    New Password Inspector Parameter File Name:




Previous Page <cntl p> Next Page <cntl n> Previous Field <cntl b>
Return to Menu <esc> Help <?>
```

Figure 4

Page 3 of the Password Inspector Form

3.3.1.12 List all Account Names Tested? (Y/N):

SPI will provide you with a listing of all the user account names it tests if you enter Y. If you enter N, this information will be excluded from the report. The initial default value for this field is Y.

3.3.1.13 List Changed Accounts? (Y/N):

Choosing the initial default value, Y, will provide you with a listing of the user accounts with passwords which have been changed from the last time the Password Inspector has been run. This option should be used in conjunction with a Password Log File (section 3.3.1.5). Otherwise, if you enter an N the final report will not contain this information.

3.3.1.14 List New Accounts? (Y/N):

SPI will provide you with a listing of any new accounts added to the password file since the last check of that file if you enter a Y. This option requires the use of a Password Log File (section 3.3.1.5). Otherwise, this information will be omitted from the final report if you enter N. The initial default value is Y.

3.3.1.15 List Passwords When Matched? (Y/N):

Choosing the initial default value, Y, will provide you with a listing of passwords which SPI has matched. If you enter N, this information will be omitted from the final report.

3.3.1.16 Save All Choices You Have Made for This Form? (Y/N):

The next time you use the Password Inspector, you may not wish to reenter all the information you have just entered. SPI will save all three pages of your current entries if you answer yes (Y) to this question. SPI will create a Password Inspector Parameter File with the name you provide in the next question. It should be something easy to remember and the maximum filename length is 21 characters. The next time you enter this form the entries you have saved will be displayed as default values.

Otherwise, if you enter N, SPI will not save your entries for this form.

3.3.1.17 New Password Inspector Parameter File Name:

If you have elected to save the entries you have made, you need to name the password inspector parameter file which SPI will create for you. The maximum filename length is 21 characters; the initial default name is **psitxmmddyy**, where the mmddyy are substituted by the numeric month, day and year respectively. Once you have finished filling out this last field of the form, this page of the form will be cleared, and the first page of the form will reappear.

In order to return to the menu, press the <escape> key.

3.3.2 Critical File Integrity Inspector Form

This form is only one page. When you are through making entries, you need to press the <escape> key to return to the menu. If you need help, **SPI** will display a help screen if you press ?. *[Help is not available as of August, 1989]*

```
                F I L E   I N T E G R I T Y   I N S P E C T O R        Page 1 of 1

     Master List File Name:                              master.list

        Edit the File? (Y/N):                            N

        Update the Entire File (snapshot)? (Y/N):        N



Previous Page <cntl p> Next Page <cntl n> Previous Field <cntl b>
Return to Menu <esc> Help <?>
```

Figure 5

File Integrity Inspector Form

You should fill in the fields of this form as follows:

Master List File Name:

The File Integrity Inspector determines if files have not changed by comparing their current checksums with a list of previously calculated checksums. Your input into this field specifies the name of the file which will be used in this comparison process. The file you specify should contain a list of file names to be compared one name on each line. Initially, the default filename is **master.list.** After you have run the File Integrity Inspector once, the default filename will be the most recent list file name entered into this field. The maximum length of an entry for this field is twenty-one characters. At this time **SPI's** user interface does not provide a mechanism for displaying the File Integrity Inspector's list file names. You can display these files by using the UNIX "ls" command in the **SPI** sub-directory *parameters/wsum.* If you enter a filename that **SPI** can not find, **SPI** will assume that you are creating a new list. The file name you enter will be used in subsequent runs of the File Integrity Inspector until it is changed. If you do not enter any file name, the cursor will remain in this field until you either specify a file name or press <escape> to return to the menu.

If you do not wish to specify a master list file name, simply press <return>. The cursor will advance to the next field, **Edit The File? (Y/N).** Press <escape> if you wish to return to the menu.

Edit the File? (Y/N):

The default value for this field is initially N. If you accept this value the cursor will advance to the last field, **Update the Entire File (snapshot)?**

If you choose Y, the form will be cleared, and the vi editor will appear with the list of file names ready for editing. You can edit this list of file names using the any of the "vi" commands. When you are through making edits, press <shift> and ZZ simultaneously. The list of file names will be saved, cleared from the screen, and the form will be displayed once again. A new checksum will be calculated and saved for any new file name in the list. This new list can then be used as the bases of future comparisons to determine if any of the files in the list have been modified. The cursor will then advance to the last field, **Update the Entire File (snapshot)?**

Update the Entire File (snapshot)? (Y/N):

The initial default value for this field is N, meaning that new checksums will not be created for all the files contained in the selected list. The first time you use **SPI** or create a new list, however, you should enter Y into this field. If you enter Y into this field, **SPI** *will* generate new checksums for each filename listed in the specified file. These starting checksums can then be used as the bases of future checks to determine if any of the files in the list have been modified. With either answer, the cursor will move back to the first field so that you can start over with another list of file names.

**** Important ****

If your list of files is long, it will take SPI a long time (possibly hours) to complete the snapshot. You will not be allowed to type anything more on this form until this task is completed.

3.3.3 Critical File Permission Inspector Form

This form is a one page form. When you are through making entries, press the <escape> key to return to the main menu. You can view a help screen by pressing ?. *[Help is not available as of August 1989].*

```
                P E R M I S S I O N   I N S P E C T O R          Page 1 of 1

      Master List File Name:                                  master.list

      Do you wish to Edit the File? (Y/N):                    N

      Do You wish to Update The Entire File (snapshot): N


Previous Page <cntl p> Next Page <cntl n> Previous Field <cntl b>
Return to Menu <esc> Help <?>
```

Figure 6

Critical File Permission Inspector Form

You should fill in the fields of this form as follows:

3.3.3.1 Master List File Name:

The Critical File Permission Inspector determines if the permissions of selected files are currently the same as contained in the previously generated permission list. Your input into the Master List File Name field determines the name of the file which contains the list of critical files to be checked. The initial default filename is **master.list**; afterwards, the default will be the list file name which you entered most recently. Entries into this field may not exceed 21 characters in length. At this time **SPI's** user interface does not provide a mechanism for displaying the Critical File Permission Inspector's list file names. You can display these files by using the UNIX "ls" command in the **SPI** sub-directory *parameters/wperm*. The file name you enter will be used in subsequent runs of the Critical File Permission Inspector, until it is changed. If you do not enter any file name, the cursor will remain in this field until you either specify a master list file name or press <escape> to return to the menu.

3.3.3.2 Do You Wish to Edit The File:

You may wish to edit the list of filenames you specified above. To do so, you need to answer yes (type a Y, then <return>) to this question, otherwise answer no (type N, then <return>). A yes answer will clear the screen and place you in the UNIX editor "vi" with the contents of the file specified above, ready to be edited. You can use any of the "vi" editor commands to add, delete or modify file names. When you are done editing, simultaneously press <shift> and ZZ. The new list of filenames will be saved and any new entries will be given the current permissions of that file. The list of file names will be saved, cleared from the screen and the form will be displayed once again. The current permissions for any new file named in the list will also be saved. This list can be used as the bases of future tests to determine if the permissions associated with any of the files in the list have changed. The cursor will then advance to the last field, **Do You Wish to Update The Entire File (snapshot).**

3.3.3.3 Do You Wish to Update The Entire File (snapshot):

The initial default value for this field is N, meaning that the current file permissions will not be used for all the files contained in the selected list. The first time you use **SPI** or create a new list, however, you should enter Y into this field. If you enter Y into this field, **SPI** *will* save the current permissions of each file named in the file specified above. The starting permissions can then be used as the bases of future checks to determine if any of the files permissions have changed. With either answer, the cursor will move back to the first field of the form, so that you can start over with another list of file names.
At this point there may be a slight delay as the **SPI** program gathers current permissions; however, the permissions snapshot runs fairly fast, and this should only take a few seconds to a minute or so.

3.3.4 Run Times Schedule

Now that you have entered the relevant parameter values for each **SPI** function you wish to use, you need to decide exactly when you want these functions to run. As mentioned previously, if you want a **SPI** function to run immediately, you need to access the main menu by pressing <escape>, then enter the number for a *run* option (e.g., RUN PERMISSION INSPECTOR, RUN FILE INTEGRITY INSPECTOR, or RUN CRITICAL FILE PERMISSION INSPECTOR).

Sometimes, however, you may not want any of **SPI's** inspectors to run immediately. In this case, select option 7 from the main menu. A **run times schedule** form will appear. This form will help you set up when you want each inspector to run. There are three notable limitations to this form. First you can only select one parameter file for each inspector. Second you can run an inspector only once a day. Third the maximum granularity for selecting a run time is one week. **SPI** does not actually keep track of the time and start a process. It simply formulates an appropriate command for the UNIX "cron" utility. The initial defaults for this form are obtained from **SPI**. Subsequent defaults are obtained from "cron". For more information on "cron" consult your UNIX manual.

This form is laid out in three sections, Run Using Which Files, Enter Run Times and Run Times. The first section is where you specify which parameter files you would like each of the inspectors to use. If you are not going to use an inspector, you do not have to specify a parameter file. If there is a default parameter file you can erase it by pressing the <backspace> key. The second section, Enter Run Times, is where you specify when you want each of the inspectors to run. The third section, Run Times, is where the run time information is displayed, it is not an input area.

```
                    R U N   T I M E S   S C H E D U L E          Page 1 of 1

 RUN USING WHICH FILES?:
 1. Password Inspector Parameter File Name:   default
 2. Permission Inspector Parameter File Name: master.list
 3. File Integrity Parameter File Name:       master.list

 ENTER RUN TIMES:
 Line(a=all)  Day(M,T,W,Th,F,S,Su)  Time(hhmm)
+-----------+---------------------+-----------+
|           |                     |     :     |
+-----------+---------------------+-----------+
| RUN TIMES                                                                  |
| Line    Function                M     T     W     Th    F     S     Su     |
| 1    Password Inspector:        :     :     :     :     :     :     :    |
| 2    Permission Inspector       :     :     :     :     :     :     :    |
| 3    File Integrity Inspector   :     :     :     :     :     :     :    |
+----------------------------------------------------------------------------+
  Save All Choices You Have Made to This Form? (Y/N): Y

Previous Page <cntl p> Next Page <cntl n> Previous Field <cntl b>
Return to Menu <esc> Help <?>
```

Figure 7
Run Times Schedule Form

3.3.4.1 Designating File Names

The first section of this form is for specifying what parameter files you want each inspector to use. These are the same parameter files you set up for each inspector (refer to the sections concerned with parameter files for each inspector). You will be asked to either accept the defaults, enter a parameter file or clear the field. You can accept the default by pressing the <return> key. If you do not want the default, simply enter the parameter file you want. The maximum number of characters you can enter is 21. SPI will check for the existence of the file and inform you if it can not find it. If you do not want to use an inspector then blank out its field by pressing the <backspace> key followed by a <return>.

3.3.4.2 Password Inspector Parameter File Name

The first parameter file you are asked for is for the Password Inspector. Either accept the default by pressing the <return> key, enter a parameter file name you have set up in option one of the menu, or blank out the field.

3.3.4.3 Permission Inspector Parameter File Name

The second field is for specifying the filename of the file that contains the list of files you want the Permission Inspector to check. These are the same files you created using option 5 of the menu. Either accept the default by pressing the <return> key, enter a file list filename, or blank out the field.

3.3.4.4 File Integrity Inspector Parameter File Name

The last field is for specifying the filename of the file that contains the list of files you want the Integrity Inspector to check. These are the same files you created using option 3 of the menu. Either accept the default by pressing the <return> key, enter a file list filename, or blank out the field.

3.3.4.5 Selecting Run Times

Next, the cursor will move to an input area immediately below the following prompt:

```
Line(a=all)   Day  (M,T,W,Th,F,S,Su)   Time(hhmm)
```

In the first leftmost box of this input area, enter the number of the particular function for which you want to set run times. Enter a number between 1 and 3 (**1** for the Password Inspector, **2** for the File Permission inspector, and **3** for the File Integrity Inspector), or enter **a** to signify that you want to set run times for *all three functions*.

After you make an entry into the first box, the cursor will subsequently move to the second box within this input area. You may designate the particular day of the week you wish **SPI** to run the function(s) you have designated in the box to the left. Type an abbreviation (**M, T, W, Th, F, S** or **Su**) for the day of the week you wish to designate.

After you have entered a day of the week, the cursor will advance to the last (rightmost) box. Type the hour (using a 24 hour clock, *from 00 to 24*) followed by a <return> and minute (00 to 59) you want **SPI** to run the task(s) you have selected into this area and then press <return>. For example, if you want a function to start at 9:20 a.m., you should type **09** <return>, then **20** <return>. (Note that the numbers you enter for the hour will be displayed on the left side of the colon which appears in this field, and the numbers which you enter for the minute will appear to the right side of the colon.) If you would like a function to start at 8:45 p.m., you should enter **20** <return>, then **45** <return> for 2045.

Remember--if you want a **SPI** function to run *right away*, you should **not** use the **Run Times Schedule** Form. You should instead exit to the menu by pressing <escape>. Then select menu options 2 (Run Permission Inspector), 4 (Run File Permission Inspector), and/or 6 (Run Critical File Integrity Inspector)!

3.3.4.6 Feedback about Times You Have Selected

After you have made entries into all three boxes, the boxes will be cleared, but your entries will be displayed below to help you keep track of what you have entered. For example, if you entered 1 in the first box, T in the second box, and 2045 in the third box, you have specified that you want the Password Inspector to run on Tuesday at 8:45 p.m. Line 1 of the display area below the input area will display the following information:

```
+-------------------------------------------------------------------------+
| RUN TIMES                                                               |
| Line    Function              M     T     W     Th    F     S     Su    |
| 1.   Password Inspector         :  20:45  :     :     :     :     :    |
| 2.   Permission Inspector       :     :   :     :     :     :     :    |
| 3.   File Integrity Inspector   :     :   :     :     :     :     :    |
+-------------------------------------------------------------------------+
```

Figure 8

Run Times Display Area

By the time you have made an entry into all three boxes, you will have informed **SPI** that you want one or more functions to run on a particular day at a particular time. However, you may want to specify different functions to run at other times. The cursor will move back to the first box, and you can make other entries. After you make three more entries (one in each box), the input area will again be cleared, and another entry will be made in the display area to show you what time you have designated.

3.3.4.7 Editing Run Times

There are two ways to edit times you have already entered. Suppose that you want to change only the hour and minute, but want to keep the function and the day of the week the same. In this case, you need to enter the number (or letter) of that function in the first box, then enter the same abbreviation for the day of the week in the second box, then enter a new time. For example, suppose you originally entered 2 (for File Permission Inspector), F (for Friday), and 1000 (for hour-minute), but now you decide that you would rather run this function at 11:30 on Friday rather than at 1000 on Friday. To make this change, you should enter **2**, then **F**, then **11** <return>, then **30** <return>. The display area will reflect this change immediately after you make it.

Another possibility is that you wish to cancel a time you have set previously. In this case, enter the code for the function (1 - 3 or a), the abbreviation for the day, and then enter 0000 for the time. For example, to clear an entry in which you previously specified that the Critical File Integrity Inspector should run at 3:00 p.m. on Wednesday, you should enter **3** in the first box, **W** in the second box, and **0000** in the third box of the input area. The entry under W in line 3 of the display area would be cleared immediately after you finished.

When you are through with your last entry, simply press <return> when the cursor is in the first box. The cursor will then move to the next field, **Save All Choices You Have Made to This Form.**

3.3.4.8 Saving Entries You Have Made

Your entry into the last field, **Save All Choices You Have Made to This Form,** determines whether or not **SPI** will save all of your current entries into the **Run Times Schedule** Form. To save all entries, you need to select the default value, Y, by pressing <return> .

Your entries will be displayed as default values the next time you access this form. Otherwise, if you enter N, **SPI** will not save your entries for this form; and the default values will not change the next time you access this form.

After you have made an entry into this field, the cursor will move to the *first field of this form*. To exit and return to the menu, press <escape>.

3.3.5 Display Output

After **SPI** has completed its inspections, you can use **SPI** to view the results. The Display Output Form is actually a menu which allows you to make this selection. This menu looks like this:

```
                    D I S P L A Y   O U T P U T                Page 1 of 1


              OUTPUT FROM WHICH FUNCTION?
                 1. Password Inspector
                 2. File Integrity
                 3. Permission Inspector

                 Enter Selection Number:


                 Name of File to View:


Previous Page <cntl p> Next Page <cntl n> Previous Field <cntl b>
Return to Menu <esc> Help <?>
```

Figure 9

Display Output Form

When you begin, the cursor will be located immediately to the right of the **Enter Selection Number** field. Select which Inspector's output you would like to view by entering a 1,2 or 3 followed by <return>.

The last field in this form is **Name of File to View.** The default is always the name of the most recent report file written. If you want to view this file, press the <return> key. Otherwise, enter the name of the report file you want to view. The format for naming report files is a two letter code followed by the date encoded in a very large number. For example, the output of the password inspector run on March, 14, 1989 at 23:26:56 will look like **ps031489232656.** These file names are not particularly easy to remember, and we will be addressing this issue in a future release of **SPI.** Each **SPI** function has its own naming convention so each function will have its own report file names (*ps* for the password inspector, *ws* for the permission inspector, and *wp* for the integrity inspector). Take heart, the report file name for a given run of a function can be found in the completion notification mail message mailed to the user specified during installation. Each function also has a special report file called cron.out. The contents of cron.out is the reports from those inspectors run from cron refer to section 3.3.4 for details on running inspectors from cron.

After you have made this specification, the file you have selected will be displayed on the screen. You will get a page at a time on the screen and to get the next page you will have to type <return> . When the file is finished, the form in figure 9 will reappear and the cursor will return to the **Enter Selection Number** field. To exit this form and return to the menu, press <escape>.

3.4 Executing SPI Functions without Menus

All **SPI** functions have a unique command name. If you wish to bypass the **SPI** menus, you simply need to edit the parameter files (if any) and then enter command names with the appropriate syntax into the UNIX shell. This is only recommended for advance UNIX system managers and computer security officers who know UNIX well. For most of the **SPI** functions to work, they require parameter files to be properly set up. All of the parameter files are in ASCII format and can be edited by the knowledgeable user. They will be found in a sub-directory called *parameters* in the **SPI** installation directory. Each function has its own sub-directory which contain those files pertinent to each function. The results of the **SPI** functions are written to *stdout.*

For example, if you set up a parameter file called *psitx* (see **SPI** UNIX Man Pages), you could access the password checker verification program by typing:

```
psi parameters/psi/psitx <return>
```

If you type:

```
vsum parameters/vsum/filelist <return>
```

you will access the program that verifies checksums for files listed in the file *filelist.* In both examples the results will be displayed on your screen.

To learn the command names for **SPI** functions, you should refer to the **SPI UNIX Man Pages.** The **SPI UNIX Man Pages** include a list of all commands related to the **SPI** program.

4. Installing SPI

Installing the **SPI** software is quite simple. Basically, the procedure is to extract the files off of the distribution media (usually magnetic tape), and to configure and build the system according to the system type and the system manager's wishes. This is handled by a program called *build*. *Build* will guide you through the building and installation of **SPI**. The *build* program will first configure SPI to run on your system. The configuration phase may seem complex, but the person installing the software only has to make a few critical decisions. Default answers to most configuration questions will be used whenever possible. After the configuration phase, *build* will compile and install the software. Before using **SPI**, the programs should be secured by setting the proper permissions. *Build* will ask you whether you want to secure the programs. YOU SHOULD ALWAYS SECURE **SPI** UNLESS YOU ARE DOING SPECIAL DEVELOPMENT WITH **SPI**. As an additional security measure, *build* will remove the source for **SPI** to protect it from compromise if your system security is breached. YOU SHOULD REMOVE THE SOURCE CODE UNLESS YOU ARE DOING SPECIAL DEVELOPMENT WITH **SPI**.

The installation procedure does not absolutely require that the installer be running as "root" or "superuser". However unless you know exactly what the installation program is doing, **we recommend that you install using root privileges**. On some systems, certain configuration questions will not work properly unless the *build* program is run from the "superuser" account. You also must be "root" to secure the **SPI** program, since permissions and ownerships need to be changed.

Before beginning the installation, you have to decide a few things about your system. Deciding these things before you begin will allow you to have the answers already determined when the *build* procedure asks you for this information.

The first piece of information you need to decide is where to extract and build **SPI**. You need about 2-3 megabytes of free space in order to build **SPI**. We recommend that you make a sub-directory in the system administrator's home directory called "spi" and build **SPI** there.

The second piece of information is where you want to put **SPI** after it has been built. The build procedure can put **SPI** anywhere, but we suggest that it be put somewhat out of the way, so casual browsers of the system are less likely to come across it. On most systems there are special places for software which isn't included with the operating system. These are usually something like "/usr/local" or "/usr/contrib". We recommend that **SPI** be installed in a sub-directory of the system administrator's account. Since **SPI** must be run as the superuser, and the installation directory is permitted only to root, it is secure in the system administrator's home directory. The default is to install **SPI** in the directory where you extracted it from the distribution.

The third piece of information is the mail address where you want **SPI** to send messages. Because most **SPI** operations take some time to complete, they are done in the background to allow you to continue with other things. When the background tasks complete, **SPI** sends mail to indicate the completion. Usually you want to send mail to the default which is "root" but you may wish to send the mail to the system administrator account or another account instead.

4.1 Step-by-Step Installation Procedure

Load the distribution media on the proper tape drive.

Change directories to the location determined in the previous section where you are going to install **SPI**. In this example we are going to install **SPI** in a sub-directory called "spi" in the system's administrator's home directory.

```
cd <return>
mkdir spi <return>
cd spi <return>
```

Extract contents of tape. (You must determine what your tape drive is called on your system.)

For 9 track magnetic tape:

```
tar xvf /dev/rmt0 <return>
```

For 1/4" cartridge tape:

```
tar xvf /dev/rst0 <return>
```

After the contents have been extracted, become "root" and run the build script and answer the questions with the default answers, or other answers as determined in previous section

```
su <return>
Password: xxxxxx <return>
build <return>
```

5. Index

6. Glossary

algorithm	A series of steps or instructions to solve a problem
alphanumeric	Referring to either alphabetical letters or numbers
character	Any of a printable set of symbols, including alphabetical characters ("a, b, c", etc.), numbers (1, 2, 3, etc.), and control characters (@, %, etc.)
Critical File Permission Inspector	A **SPI** function which checks for discrepancies between actual and recommended file permissions
crypto-checksum	A mathematical operation to check the contents of a file which produces a unique number based on a cryptological algorithm--any change to the contents of a file will virtually always cause a change to the crypto-checksum, enabling one to readily detect a modification to a file
default	A value which is given by the system, such that if the user does not enter another value, the system accepts this value as the value supplied by the user
enter	To input one or more characters, then press <return>
/etc/passwd	The UNIX password file (which lists passwords for system accounts)
field	An area, usually within a displayed form, where the user can read and/or input values
field heading	A label for a field, which enables the user to determine what kind of information is contained in that field
File Integrity Inspector	A **SPI** function which determines whether the file being inspected has changed contents since the last time it was compared against a checksum list.
function	A program within **SPI** designed to accomplish some task for the user, such as checking file permissions
GCOS field	A field of the password file which contains information such as the full name, phone number, etc. of the person holding an account on the system
man pages	See **SPI** UNIX Man Pages

menu driven	A style of interacting with a system in which options are displayed, and the user enters a code to select one of these options
on-line	Pertaining to events under the control of the computer, which responds directly and immediately to user commands
Password Inspector	A **SPI** function which checks the password file or any other file designated by the system manager that contains the same format as the password file.
permutations	Unique orderings of elements such as character strings
root account	The account of a "super-user," allowing special privileges to the user
root privileges	"Super-user" privileges, including ability to read and write to all system files, access to all accounts, etc.
Security Profile Inspector	A set of programs which analyze aspects of a system such as the passwords and file integrity to determine how vulnerable that system is to intrusion.
SPI	Security Profile Inspector
SPI UNIX Man Pages	On-line help for UNIX systems--command is man (topic), and it displays pages from the User Manual
system manager	Someone who takes care of the details of keeping a systems hardware and software running, and helping users when they need help--they do backups
UNIX	A commonly used operating system developed at AT&T--known for its ease of use in building software and portability of software
UNIX shell	A program that interprets all the commands the user enters
VT100 terminal	A terminal built by the Digital Equipment Corporation which has a 24-line, 80-column text display capability
VT100 emulation	Software which duplicates the characteristics of a VT100 terminal. Software which is made to run on a VT100 terminal can also run on another type of terminal if VT100 emulation software is used