SECURATE QUICK REFERENCE GUIDE

THE LANGUAGE

Primary Terms

high
low
medium

Primary Hedges

extremely
very
pretty
fairly
sortof

Relations

lower than
higher than

Relation Hedges

not
much
slightly

Connectives

and
to

Additionally, a number from one to ten may be specified, optionally preceded by "**about**". If a number is used, it must be spelled out in letters.

DATA ENTRY

The following commands may be entered following a ":" prompt:

ADD <object name>
VALUE <object value>
NEXT
OFFSPRING
OUT

With the exception of **OUT**, the above commands may be shortened to the first letter.

SECURITY EVALUATION FUNCTIONS

The following commands may be entered:

OVERALLRATING (or ORATE)
INDIVIDUALRATING (or IRATE)
SECTIONALRATING (or SRATE)
WORSTSUBSECTION (or WRATE)

Scoring Options

The following scoring options are available and may be specified by entering either "**SETRATE**", followed by a prompt, or just "**RATESET**":

1) Weakest Link
2) Selected Weakest Link
3) Fuzzy Mean
4) Weighted Fuzzy Mean
5) Fuzzy Mean With Each Major Subsection Weighted By Maximum Object Value

Other Functions

ADDTRIP
DELTRIP
MODTRIP
SAVE
HIERARCHY
THREATS
FEATURES

SECURATE User's Manual

by

Lance J. Hoffman, Eric H. Michelman, and Don Clements

Memorandum No. UCB/ERL M77/49

21 July 1977

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

SECURATE User's Manual

TABLE OF CONTENTS

Research sponsored by National Science Foundation Grant MCS76-09214.

1. INTRODUCTION

This manual provides instructions for using SECURATE, an interactive security evaluation and analysis system. SECURATE was designed to analyze computer installations, but it is easily adapted to other security options. The user first inputs the data necessary to describe the installation from a security point of view. A set of security evaluation functions are then provided to assist the user in analyzing the installation's security.

The installation is described as a set of object-threat-feature triples. OBJECTS are defined as the resources within a computing system, the loss of which would have a cost to the owner. THREATS are activities which a potential intruder may employ to gain unauthorized access to an object. This term also refers to chance events which may jeopardize an object. FEATURES are protective measures which present some degree of resistance to a threat.

The system incorporates a hierarchical structure of objects commonly found in computer installations. Associated with the object hierarchy is a listing of corresponding threats and security features. A portion of the object hierarchy is illustrated in figure 1.1. The entire object hierarchy and threat and feature listings are given in Appendix A. The hierarchy is used extensively throughout the system to structure both the analysis and the data input.

Each triple is specified by the user in terms of object value, threat likelihood, and feature resistance. A key feature of this system is that the measures of object value, threat likelihood and feature resistance, as well as the resultant security rating, are specified in terms of linguistic variables--variables which assume values which are words rather than numbers. Acceptable values are words such as **high**, **low**, and **medium**. Appropriate modifiers provide finer resolution by allowing terms such as **very high**, **somewhat high**, **medium to high**, etc.

The user thus describes the installation by specifying triples composed of object value, threat likelihood, and feature resistance. An input program leads the user through the object hierarchy, allowing him to modify the hierarchy to fit the particular installation and to specify appropriate triples. Security evaluation functions are then supplied which take the set of triples as input and return security ratings. Subsets of the triples set, corresponding to subsections of the hierarchy, can also be rated. For example one might elect to rate only the CENTRAL MACHINE subsection of figure 1.1. An informational facility is also available for suggesting security threats and measures.

- 1. Hardware
  - 1.1 Central machine
    - 1.1.1 CPU
    - 1.1.2 Main memory
    - 1.1.3 I/O channels
    - 1.1.4 Operator's console
  - 1.2 Storage medium
    - 1.2.1 Magnetic media
      - 1.2.1.1 Disk packs
      - 1.2.1.2 Magnetic tapes
      - 1.2.1.3 Diskettes (floppies)
      - 1.2.1.4 Cassettes
      - 1.2.1.5 Other
    - 1.2.2 Non-magnetic media
      - 1.2.2.1 Punched cards
      - 1.2.2.2 Paper tape
      - 1.2.2.3 Paper printout
      - 1.2.2.4 Other
  - 1.3 Communications equipment
    - 1.3.1 Communications lines
    - 1.3.2 Communications processor
    - 1.3.3 Multiplexor
  - 1.4 I/O devices
    - 1.4.1 User directed I/O devices
      - 1.4.1.1 Printer
      - 1.4.1.2 Card reader
      - 1.4.1.3 Card punch
      - 1.4.1.4 Paper tape reader
      - 1.4.1.5 Paper tape punch
      - 1.4.1.6 Terminals
        - 1.4.1.6.1 Local terminals
        - 1.4.1.6.2 Remote terminals
      - 1.4.1.7 Modems
    - 1.4.2 Storage I/O devices
      - 1.4.2.1 Disk drives
      - 1.4.2.2 Tape drives

Figure 1.1 Portion of the Object Hierarchy

2. THE LANGUAGE

2.1 The Language Terms

Presently, the following terms are available for use in specifying the object values, threat likelihoods, and feature resistances:

Primary Terms	*Primary Hedges*	*Relations*
high	**extremely**	**lower than**
low	**very**	**higher than**
medium	**pretty**	
	fairly	
	sortof	

Relation Hedges	*Connectives*
not	**and**
much	**to**
slightly	

Additionally, a number from one to ten may be specified, optionally preceded by a blank. If a number is used, it must be spelled out in letters.

2.2 Examples

Following are examples of acceptable phrases:

high
low
medium
very high
moreorless medium
fairly low
low to medium
(about four) to about six
slightly lower than pretty high
not higher than medium
(much higher than low) and slightly lower than sortof medium

The following phrases are not acceptable:

extremely (a primary term--"**high**", "**low**", or "**medium**"--must be used)

not very (a primary term must be used)

about high ("**about**" may only modify numbers)

5 (numbers must be spelled out, e.g. "**five**")

slightly high ("**slightly**" is a relation hedge, which may only modify "**lower than**" or "**higher than**")

slightly higher than medium and lower than pretty high (parenthesis must enclose two or more words to the left of "**and**" or "**to**")

2.3 Hedges

The words "**extremely**" and "**very**" sharpen the curve toward the extreme, "**extremely**" more so than "**very**".

The words "**sortof**", "**fairly**", and "**pretty**" shift the curve toward the middle, "**sortof**" shifting it the most, and "**pretty**" shifting it the least.

2.4 Rules of Use

Basically, anything that sounds like English is acceptable. However, following is a set of simple rules:

1) At least one primary term must be present.

2) Primary hedges modify primary terms.

3) Relations modify primary terms or a combination of a primary term and a primary hedge.

4) Relation hedges modify relations.

5) Connectives connect any two of the above forms.

6) Anything to the left of a connective must be enclosed in parenthesis if it is more than one word.

Appendix C contains a formal definition of the language.

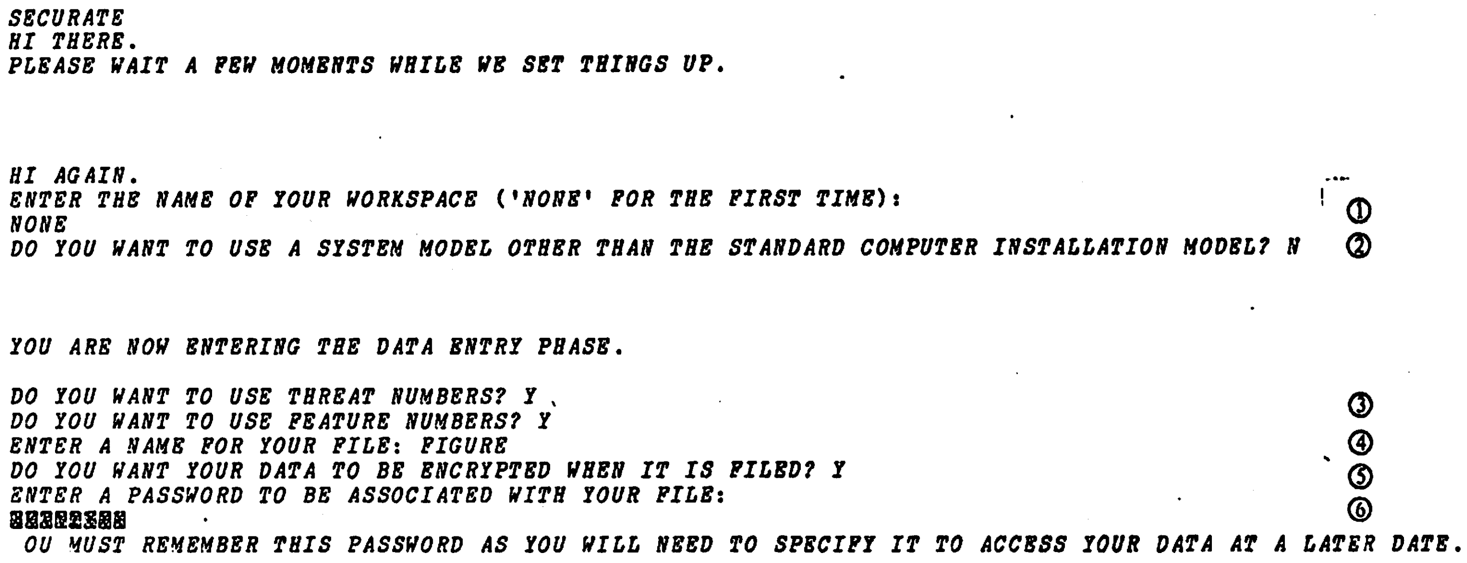
3. INITIALIZATION AND DATA ENTRY

3.1 Initialization

SECURATE is called by entering "SECURATE" after logon. Instruction for logging on and off are given in Appendix E.

Before data entry can begin, the user must make some initialization choices.

Figure 3.1 shows an example of this portion of the terminal session when SECURATE is first used.



```
SECURATE
HI THERE.
PLEASE WAIT A FEW MOMENTS WHILE WE SET THINGS UP.


HI AGAIN.
ENTER THE NAME OF YOUR WORKSPACE ('NONE' FOR THE FIRST TIME):                                    ①
NONE
DO YOU WANT TO USE A SYSTEM MODEL OTHER THAN THE STANDARD COMPUTER INSTALLATION MODEL? N          ②


YOU ARE NOW ENTERING THE DATA ENTRY PHASE.

DO YOU WANT TO USE THREAT NUMBERS? Y                                                              ③
DO YOU WANT TO USE FEATURE NUMBERS? Y
ENTER A NAME FOR YOUR FILE: FIGURE                                                                ④
DO YOU WANT YOUR DATA TO BE ENCRYPTED WHEN IT IS FILED? Y                                         ⑤
ENTER A PASSWORD TO BE ASSOCIATED WITH YOUR FILE:
▓▓▓▓▓▓▓▓                                                                                          ⑥
 OU MUST REMEMBER THIS PASSWORD AS YOU WILL NEED TO SPECIFY IT TO ACCESS YOUR DATA AT A LATER DATE.
```

Figure 3.1 Initialization sequence

The user is first asked for the name of his workspace (file), being directed to enter "none" if this is the first time the system is being used (refer to point ①, figure 3.2).

Next, the user is asked if he wants to use the computer installation model or one of the other models available ②. The models are all structured similarly; only the actual objects, threats, and features differ. A list if all available models is given in Appendix D.

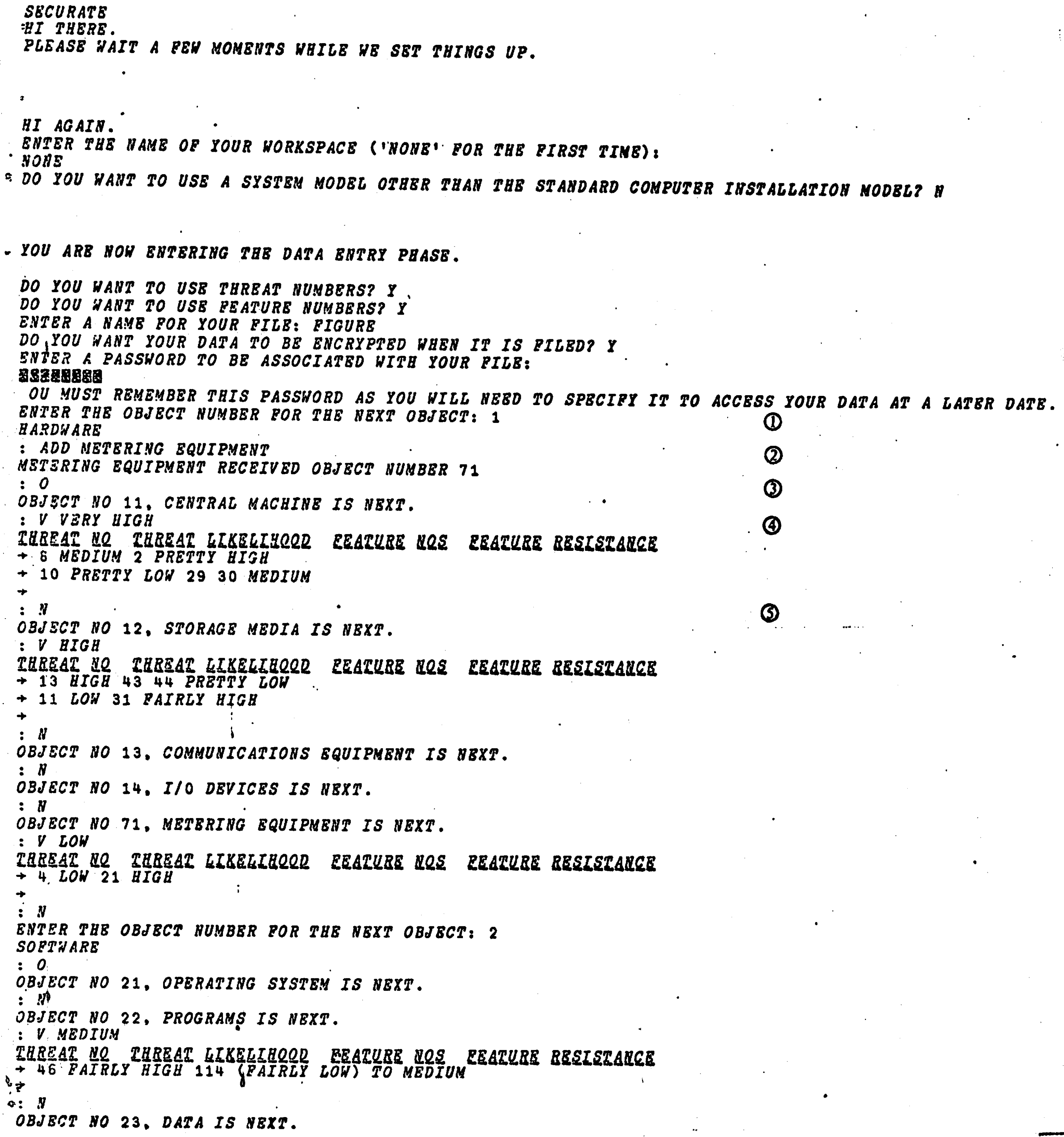
Once the installation model is set up, the user is given the option of associating a threat and/or feature number with each triple ③. These numbers are solely for identification purposes; no analysis functions consider them. The number may refer to the lists of threats and features associated with the object hierarchy, or may be numbers chosen by the user according to his own numbering scheme. If a threat or feature number used is one of those in the threat or feature listings (nos. 1-129 for threats and nos. 1-274 for features), the corresponding name will be printed out by the display function.

The user is next asked for a name for the file that will contain his data ④. He will then be asked if the data should be encrypted ⑤, and, if so, a password to base the encryption on (we suggest at least four characters which the user can remember) ⑥. Encryption is recommended if the information entered as triples is sensitive, as little other protection is provided.

3.2 Data Entry

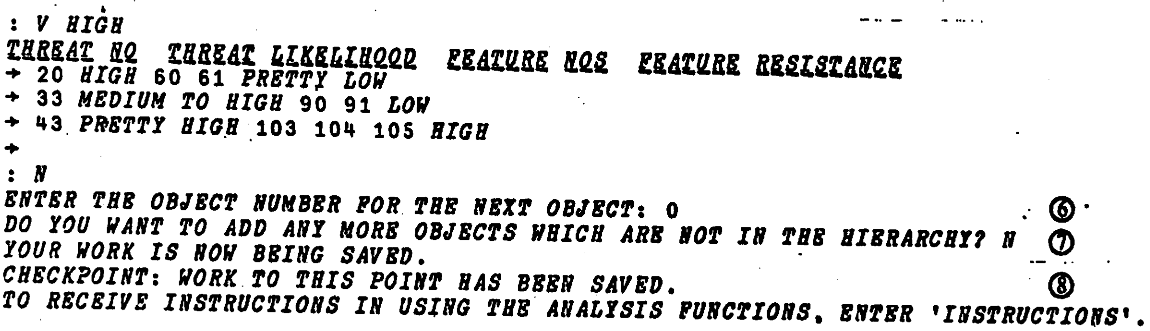
After initialization, as described in section 3.1, the user is ready to begin data entry. In entering the data, the user is led though the hierarchy, being given the opportunity at each node to add offspring or specify triples for that object. The system will prompt for the first object (refer to point ①, figure 3.2).

Figure 3.2 illustrates a typical terminal session of inputing data and the resultant output from the display function.



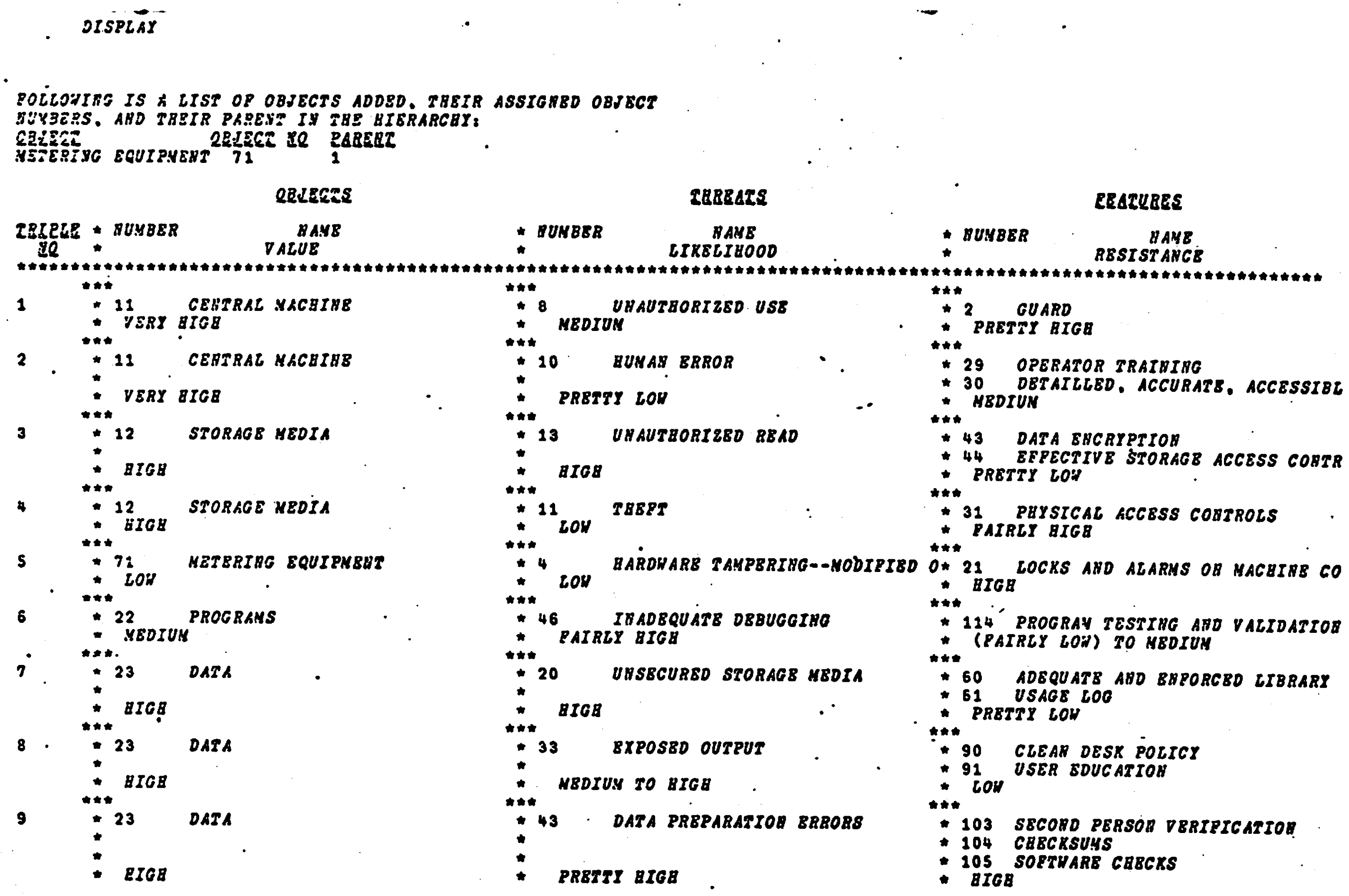
```
SECURATE
HI THERE.
PLEASE WAIT A FEW MOMENTS WHILE WE SET THINGS UP.


HI AGAIN.
ENTER THE NAME OF YOUR WORKSPACE ('NONE' FOR THE FIRST TIME):
NONE
DO YOU WANT TO USE A SYSTEM MODEL OTHER THAN THE STANDARD COMPUTER INSTALLATION MODEL? N


YOU ARE NOW ENTERING THE DATA ENTRY PHASE.

DO YOU WANT TO USE THREAT NUMBERS? Y
DO YOU WANT TO USE FEATURE NUMBERS? Y
ENTER A NAME FOR YOUR FILE: FIGURE
DO YOU WANT YOUR DATA TO BE ENCRYPTED WHEN IT IS FILED? Y
ENTER A PASSWORD TO BE ASSOCIATED WITH YOUR FILE:
[redacted]
 OU MUST REMEMBER THIS PASSWORD AS YOU WILL NEED TO SPECIFY IT TO ACCESS YOUR DATA AT A LATER DATE.
ENTER THE OBJECT NUMBER FOR THE NEXT OBJECT: 1
HARDWARE                                                                          ①
: ADD METERING EQUIPMENT                                                          ②
METERING EQUIPMENT RECEIVED OBJECT NUMBER 71
: O                                                                               ③
OBJECT NO 11, CENTRAL MACHINE IS NEXT.
: V VERY HIGH                                                                     ④
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
→ 6 MEDIUM 2 PRETTY HIGH
→ 10 PRETTY LOW 29 30 MEDIUM
→
: N                                                                               ⑤
OBJECT NO 12, STORAGE MEDIA IS NEXT.
: V HIGH
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
→ 13 HIGH 43 44 PRETTY LOW
→ 11 LOW 31 FAIRLY HIGH
→
: N
OBJECT NO 13, COMMUNICATIONS EQUIPMENT IS NEXT.
: N
OBJECT NO 14, I/O DEVICES IS NEXT.
: N
OBJECT NO 71, METERING EQUIPMENT IS NEXT.
: V LOW
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
→ 4 LOW 21 HIGH
→
: N
ENTER THE OBJECT NUMBER FOR THE NEXT OBJECT: 2
SOFTWARE
: O
OBJECT NO 21, OPERATING SYSTEM IS NEXT.
: N
OBJECT NO 22, PROGRAMS IS NEXT.
: V MEDIUM
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
→ 46 FAIRLY HIGH 114 (FAIRLY LOW) TO MEDIUM
→
: N
OBJECT NO 23, DATA IS NEXT.
```

Figure 3.2a Inputing the data



```
: V HIGH
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
→ 20 HIGH 60 61 PRETTY LOW
→ 33 MEDIUM TO HIGH 90 91 LOW
→ 43 PRETTY HIGH 103 104 105 HIGH
→
: N
ENTER THE OBJECT NUMBER FOR THE NEXT OBJECT: 0                            ⑥
DO YOU WANT TO ADD ANY MORE OBJECTS WHICH ARE NOT IN THE HIERARCHY? N     ⑦
YOUR WORK IS NOW BEING SAVED.
CHECKPOINT: WORK TO THIS POINT HAS BEEN SAVED.                            ⑧
TO RECEIVE INSTRUCTIONS IN USING THE ANALYSIS FUNCTIONS, ENTER 'INSTRUCTIONS'.
```

Figure 3.2a continued



```
DISPLAY

FOLLOWING IS A LIST OF OBJECTS ADDED, THEIR ASSIGNED OBJECT
NUMBERS, AND THEIR PARENT IN THE HIERARCHY:
OBJECT             OBJECT NO   PARENT
METERING EQUIPMENT  71          1

                       OBJECTS                                      THREATS                                     FEATURES

TRIPLE * NUMBER           NAME             * NUMBER        NAME               * NUMBER         NAME
  NO   *                 VALUE             *             LIKELIHOOD           *             RESISTANCE
*************************************************************************************************************************
       ***                                 ***                                ***
1      * 11     CENTRAL MACHINE            * 8      UNAUTHORIZED USE          * 2    GUARD
       *  VERY HIGH                        *  MEDIUM                          *  PRETTY HIGH
       ***                                 ***                                ***
2      * 11     CENTRAL MACHINE            * 10     HUMAN ERROR               * 29   OPERATOR TRAINING
       *                                   *                                  * 30   DETAILLED, ACCURATE, ACCESSIBL
       *  VERY HIGH                        *  PRETTY LOW                      *  MEDIUM
       ***                                 ***                                ***
3      * 12     STORAGE MEDIA              * 13     UNAUTHORIZED READ         * 43   DATA ENCRYPTION
       *                                   *                                  * 44   EFFECTIVE STORAGE ACCESS CONTR
       *  HIGH                             *  HIGH                            *  PRETTY LOW
       ***                                 ***                                ***
4      * 12     STORAGE MEDIA              * 11     THEFT                     * 31   PHYSICAL ACCESS CONTROLS
       *  HIGH                             *  LOW                             *  FAIRLY HIGH
       ***                                 ***                                ***
5      * 71     METERING EQUIPMENT         * 4      HARDWARE TAMPERING--MODIFIED O* 21   LOCKS AND ALARMS ON MACHINE CO
       *  LOW                              *  LOW                             *  HIGH
       ***                                 ***                                ***
6      * 22     PROGRAMS                   * 46     INADEQUATE DEBUGGING      * 114  PROGRAM TESTING AND VALIDATION
       *  MEDIUM                           *  FAIRLY HIGH                     *  (FAIRLY LOW) TO MEDIUM
       ***                                 ***                                ***
7      * 23     DATA                       * 20     UNSECURED STORAGE MEDIA   * 60   ADEQUATE AND ENFORCED LIBRARY
       *                                   *                                  * 61   USAGE LOG
       *  HIGH                             *  HIGH                            *  PRETTY LOW
       ***                                 ***                                ***
8      * 23     DATA                       * 33     EXPOSED OUTPUT            * 90   CLEAN DESK POLICY
       *                                   *                                  * 91   USER EDUCATION
       *  HIGH                             *  MEDIUM TO HIGH                  *  LOW
       ***                                 ***                                ***
9      * 23     DATA                       * 43     DATA PREPARATION ERRORS   * 103  SECOND PERSON VERIFICATION
       *                                   *                                  * 104  CHECKSUMS
       *                                   *                                  * 105  SOFTWARE CHECKS
       *  HIGH                             *  PRETTY HIGH                     *  HIGH
```

Figure 3.2b Output from DISPLAY

For each object considered, the user may perform the functions described below. The system will prompt the user with a colon, ":", when it is ready to accept these commands.

ADD--this will add offspring to an object. This is used to insert other objects into the hierarchy under the object presently being considered. To do this, enter "ADD" followed by the name of the object to be added ②.

VALUE--to enter triples for the object presently under consideration, start by typing "VALUE" followed by the object value ④. The header

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

will then be printed out and the information for each triple for that object may be entered, one triple to an input line. The system will prompt the user with a right pointing arrow, "→", prior to each line entered in this phase. The object value will be that specified following the VALUE keyword. If the user chooses not to use either threat or feature numbers, the corresponding part of the header does not appear. If feature numbers are specified, no punctuation can be used to separate the entries; otherwise the threat likelihood and feature resistance must be separated by a comma. When all of the triples information has been entered for the object, enter a blank carriage return. At this point, the user may specify more triples for the same object, but a different object value, or may use one of the control functions described below to move on to another object. While it is unusual to consider two different object values for the same object, it is occasionally appropriate. An example of this would be specifying a LOW value for a sensitive data file when the threat is accidental erasure (assuming a backup copy exists) and specifying a HIGH value when the threat is unauthorized access.

In addition to the functions above, the following control commands may be entered:

NEXT--the system will continue by prompting the user with the previous object's siblings, or, if none, ask the user for the next object number ⑤.

OFFSPRING--the system will continue by prompting the user with the previous object's offspring, or, if none, its siblings ③. If there are no offspring or siblings, the user will be asked for the next object number.

OUT--exit from the program (for exiting from the system, see Appendix E for logoff instructions.)

With the exception of OUT, the above commands may be shortened to the first letter.

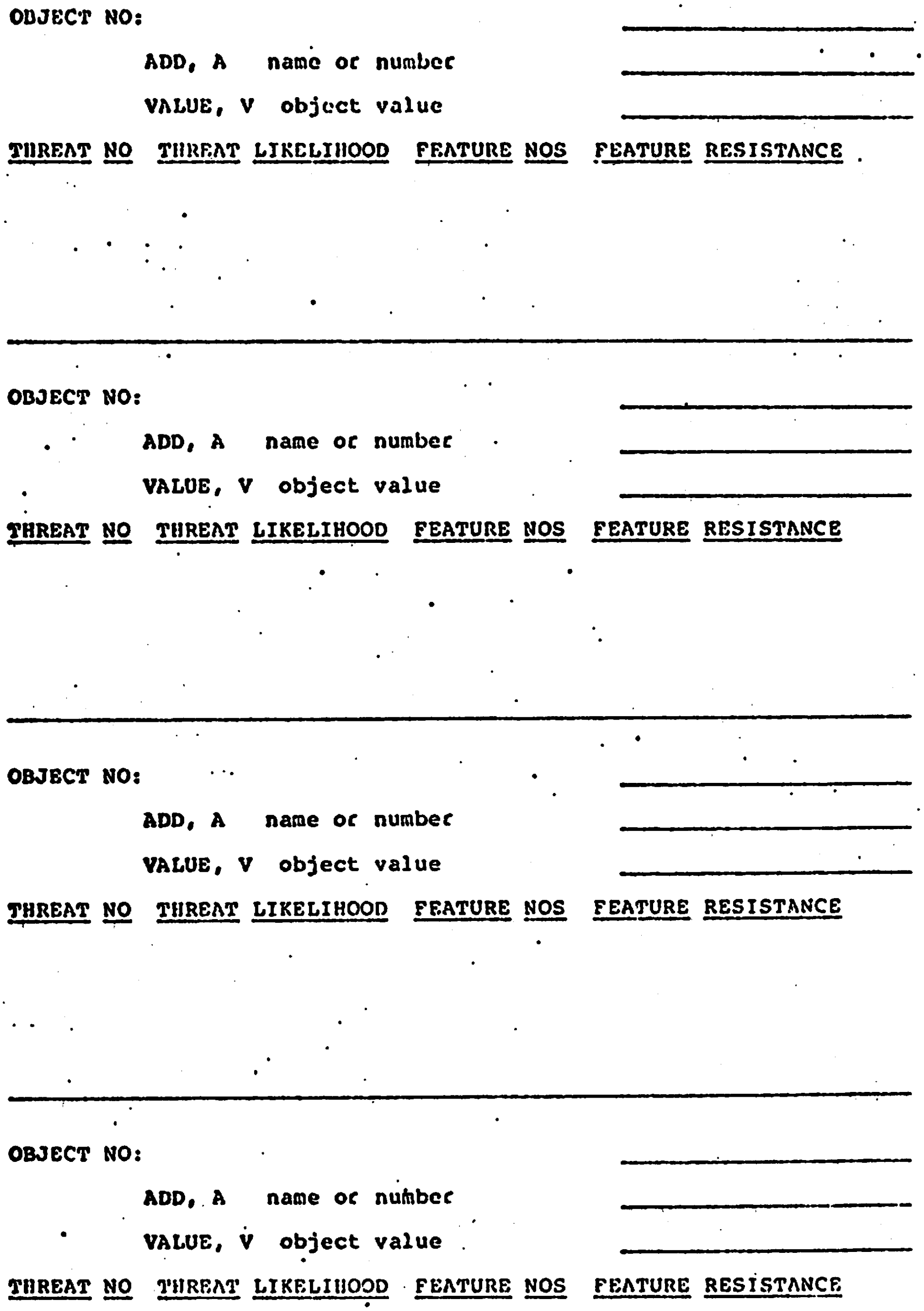
Note that when a ":" is used as a prompt, the system is expecting a command--ADD, VALUE, NEXT, OFFSPRING, or OUT. When a "→" is used as a prompt, the system is operating under the VALUE command, and it is expecting a line of triples' information (threat no., threat likelihood, feature no., feature resistance). To switch from the later, "→", to the former, ":", enter a blank line (just a carriage return).

To add objects outside of the hierarchy, enter a 0 at a point when the system is asking for the next object number ⑥. This should also be done to exit from the program at that point, responding "NO" to the prompt concerning adding objects ⑦.

To use the data entry program at a later time, enter "SETMODEL", calling the function of that name which will accept more input of the same form.

During the data entry, the current workspace is periodicaly saved to guard against a computer system crash. Each time this is completed, the message "CHECKPOINT: WORK TO THIS POINT HAS BEEN SAVED." is printed at the terminal ⑧.

When gathering the data it is suggested that the user use photostats of the form in Appendix B. Figure 3.3 illustrates both a blank form and completed forms corresponding to the data input of figure 3.2. Note that the order of the objects on the forms is such that each object is immediately followed by its offspring. This is the easiest way to go through the hierarchy when entering triples.



OBJECT NO: ____________________

ADD, A name or number ____________________

VALUE, V object value ____________________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

OBJECT NO: ____________________

ADD, A name or number ____________________

VALUE, V object value ____________________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

OBJECT NO: ____________________

ADD, A name or number ____________________

VALUE, V object value ____________________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

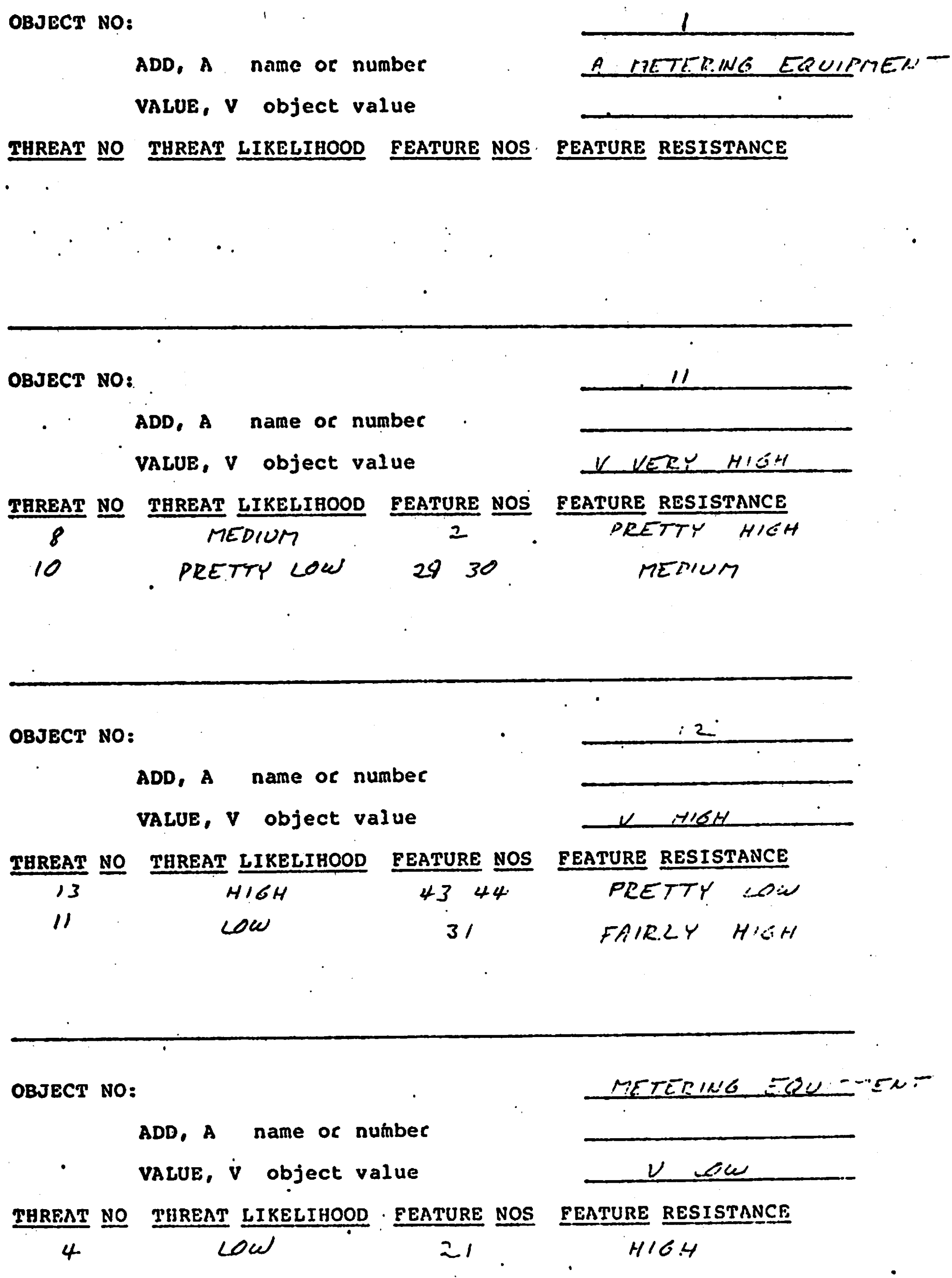
OBJECT NO: ____________________

ADD, A name or number ____________________

VALUE, V object value ____________________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

Figure 3.3a A blank input form



OBJECT NO: 1

ADD, A name or number A METERING EQUIPMENT

VALUE, V object value

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

OBJECT NO: 11

ADD, A name or number

VALUE, V object value V VERY HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
8	MEDIUM	2	PRETTY HIGH
10	PRETTY LOW	29 30	MEDIUM

OBJECT NO: 12

ADD, A name or number

VALUE, V object value V HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
13	HIGH	43 44	PRETTY LOW
11	LOW	31	FAIRLY HIGH

OBJECT NO: METERING EQUIPMENT

ADD, A name or number

VALUE, V object value V LOW

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
4	LOW	21	HIGH

Figure 3.3b Input form completed before logging on

OBJECT NO: 22

ADD, A name or number

VALUE, V object value V MEDIUM

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
46	FAIRLY HIGH	114	(FAIRLY LOW) TO MEDIUM

OBJECT NO: 23

ADD, A name or number

VALUE, V object value V HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
20	HIGH	60 61	PRETTY LOW
33	MEDIUM TO HIGH	90 91	LOW
43	PRETTY HIGH	103 104 105	HIGH

OBJECT NO:

ADD, A name or number

VALUE, V object value

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE

OBJECT NO:

ADD, A name or number

VALUE, V object value

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE

Figure 3.3b cont. Second completed input form

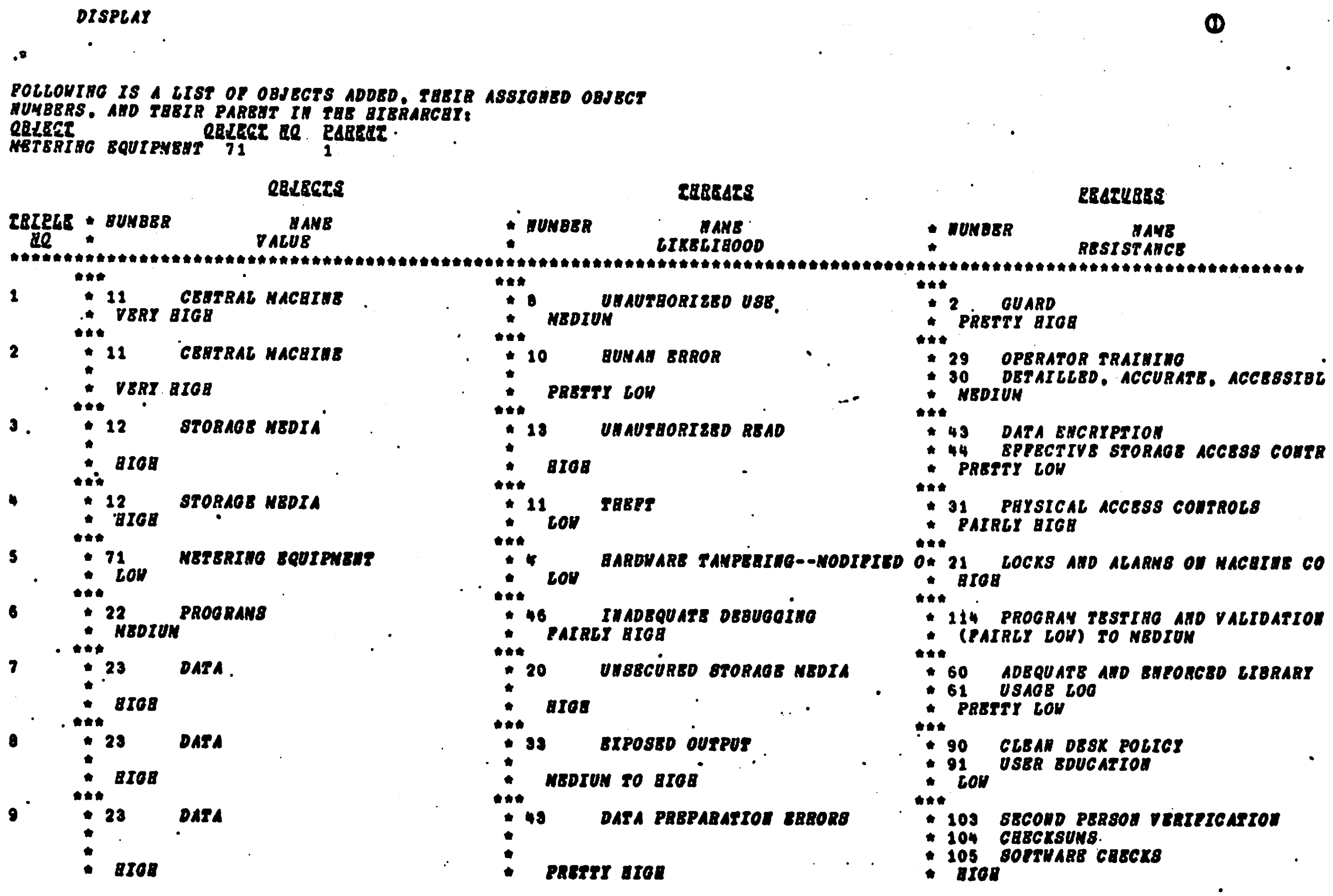
4. USE OF THE ANALYSIS FUNCTIONS

Once the triples information has been entered, the analysis functions may be used.

There are presently two types of analysis functions available, security evaluation functions and informational functions. They may be invoked interchangeably.

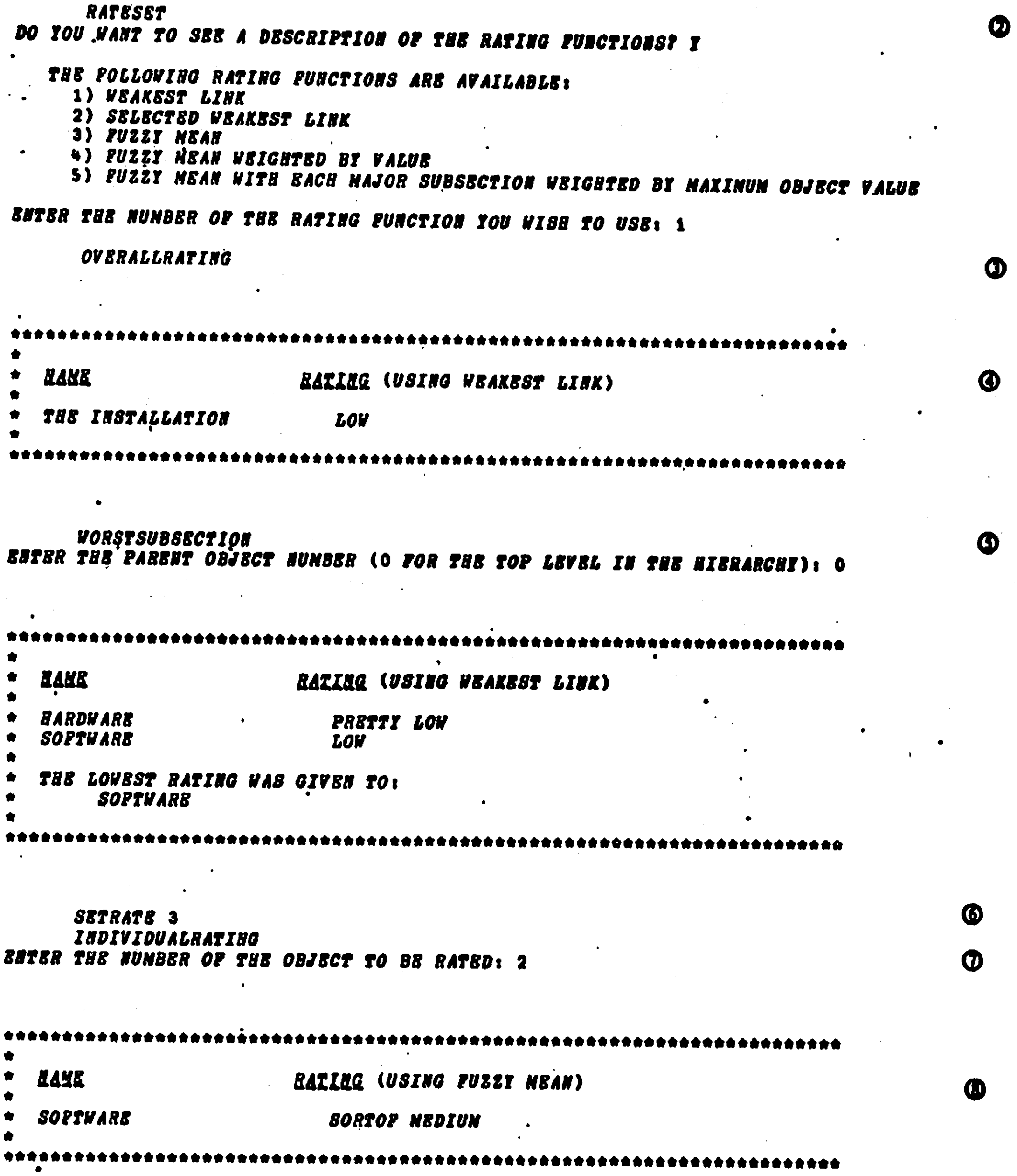
4.1 Security Evaluation Functions

Figure 4.1 illustrates the use of the security evaluation functions with the different rating options. Both the functions and the options will be described following figure 4.1. The data used is the data input in figure 3.2.



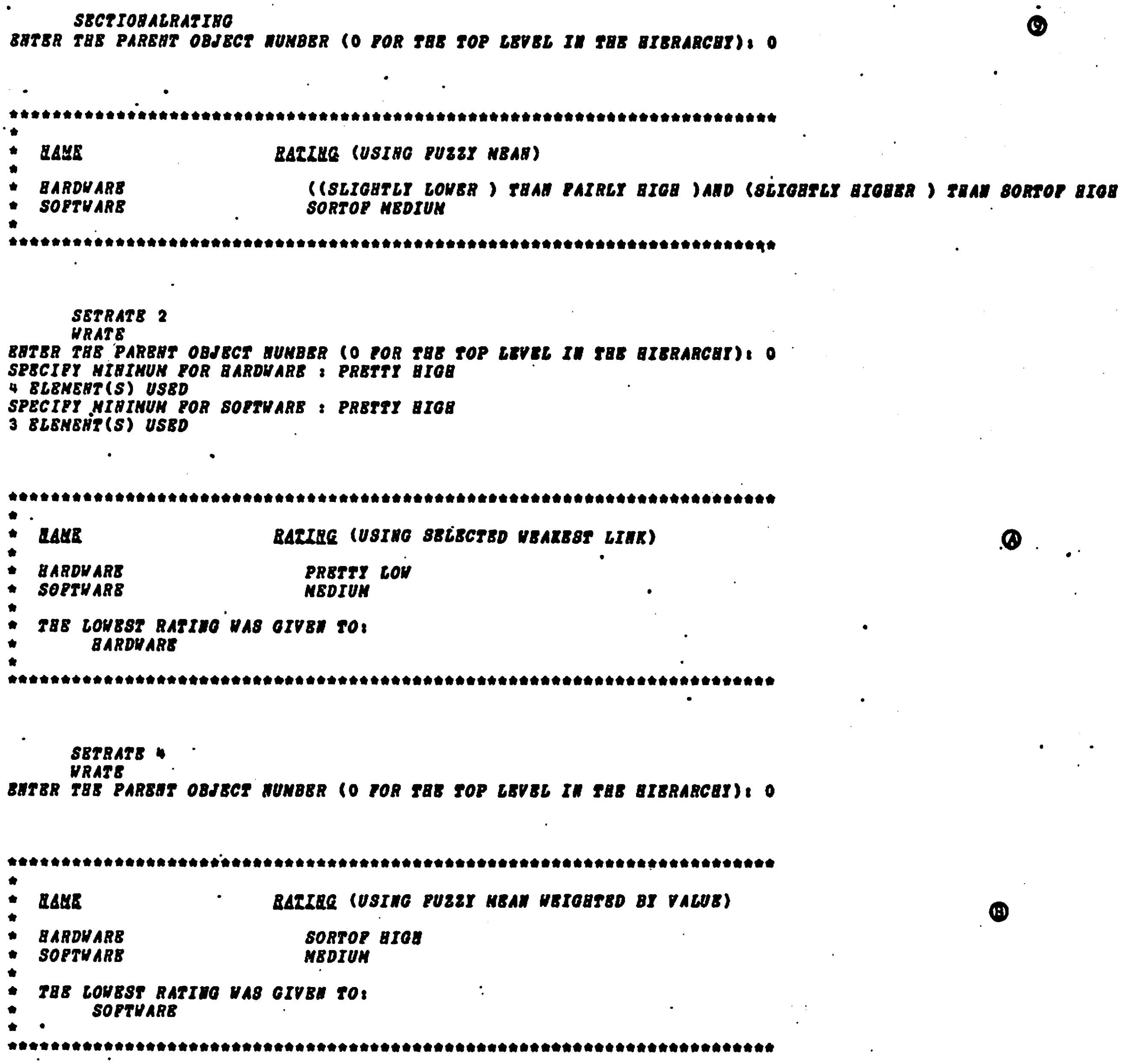
```
     DISPLAY


FOLLOWING IS A LIST OF OBJECTS ADDED, THEIR ASSIGNED OBJECT
NUMBERS, AND THEIR PARENT IN THE HIERARCHY:
OBJECT              OBJECT NO  PARENT
METERING EQUIPMENT  71         1

                         OBJECTS                                        THREATS                                        FEATURES

TRIPLE * NUMBER              NAME                  * NUMBER          NAME                       * NUMBER              NAME
 NO    *                    VALUE                  *              LIKELIHOOD                    *                  RESISTANCE
******************************************************************************************************************************
      ***                                          ***                                          ***
1      * 11      CENTRAL MACHINE                   * 8       UNAUTHORIZED USE                   * 2    GUARD
       *  VERY HIGH                                *   MEDIUM                                   *  PRETTY HIGH
      ***                                          ***                                          ***
2      * 11      CENTRAL MACHINE                   * 10      HUMAN ERROR                        * 29   OPERATOR TRAINING
       *                                           *                                            * 30   DETAILLED, ACCURATE, ACCESSIBL
       *  VERY HIGH                                *   PRETTY LOW                               *  MEDIUM
      ***                                          ***                                          ***
3      * 12      STORAGE MEDIA                     * 13      UNAUTHORIZED READ                  * 43   DATA ENCRIPTION
       *                                           *                                            * 44   EFFECTIVE STORAGE ACCESS CONTR
       *  HIGH                                     *   HIGH                                     *  PRETTY LOW
      ***                                          ***                                          ***
4      * 12      STORAGE MEDIA                     * 11      THEFT                              * 31   PHYSICAL ACCESS CONTROLS
       *  HIGH                                     *   LOW                                      *  FAIRLY HIGH
      ***                                          ***                                          ***
5      * 71      METERING EQUIPMENT                * 4       HARDWARE TAMPERING--MODIFIED O* 21   LOCKS AND ALARMS ON MACHINE CO
       *  LOW                                      *   LOW                                      *  HIGH
      ***                                          ***                                          ***
6      * 22      PROGRAMS                          * 46      INADEQUATE DEBUGGING               * 114  PROGRAM TESTING AND VALIDATION
       *  MEDIUM                                   *   FAIRLY HIGH                              *  (FAIRLY LOW) TO MEDIUM
      ***                                          ***                                          ***
7      * 23      DATA                              * 20      UNSECURED STORAGE MEDIA            * 60   ADEQUATE AND ENFORCED LIBRARY
       *                                           *                                            * 61   USAGE LOG
       *  HIGH                                     *   HIGH                                     *  PRETTY LOW
      ***                                          ***                                          ***
8      * 23      DATA                              * 33      EXPOSED OUTPUT                     * 90   CLEAN DESK POLICY
       *                                           *                                            * 91   USER EDUCATION
       *  HIGH                                     *   MEDIUM TO HIGH                           *  LOW
      ***                                          ***                                          ***
9      * 23      DATA                              * 43      DATA PREPARATION ERRORS            * 103  SECOND PERSON VERIFICATION
       *                                           *                                            * 104  CHECKSUMS
       *                                           *                                            * 105  SOFTWARE CHECKS
       *  HIGH                                     *   PRETTY HIGH                              *  HIGH
```

Figure 4.1a The data display



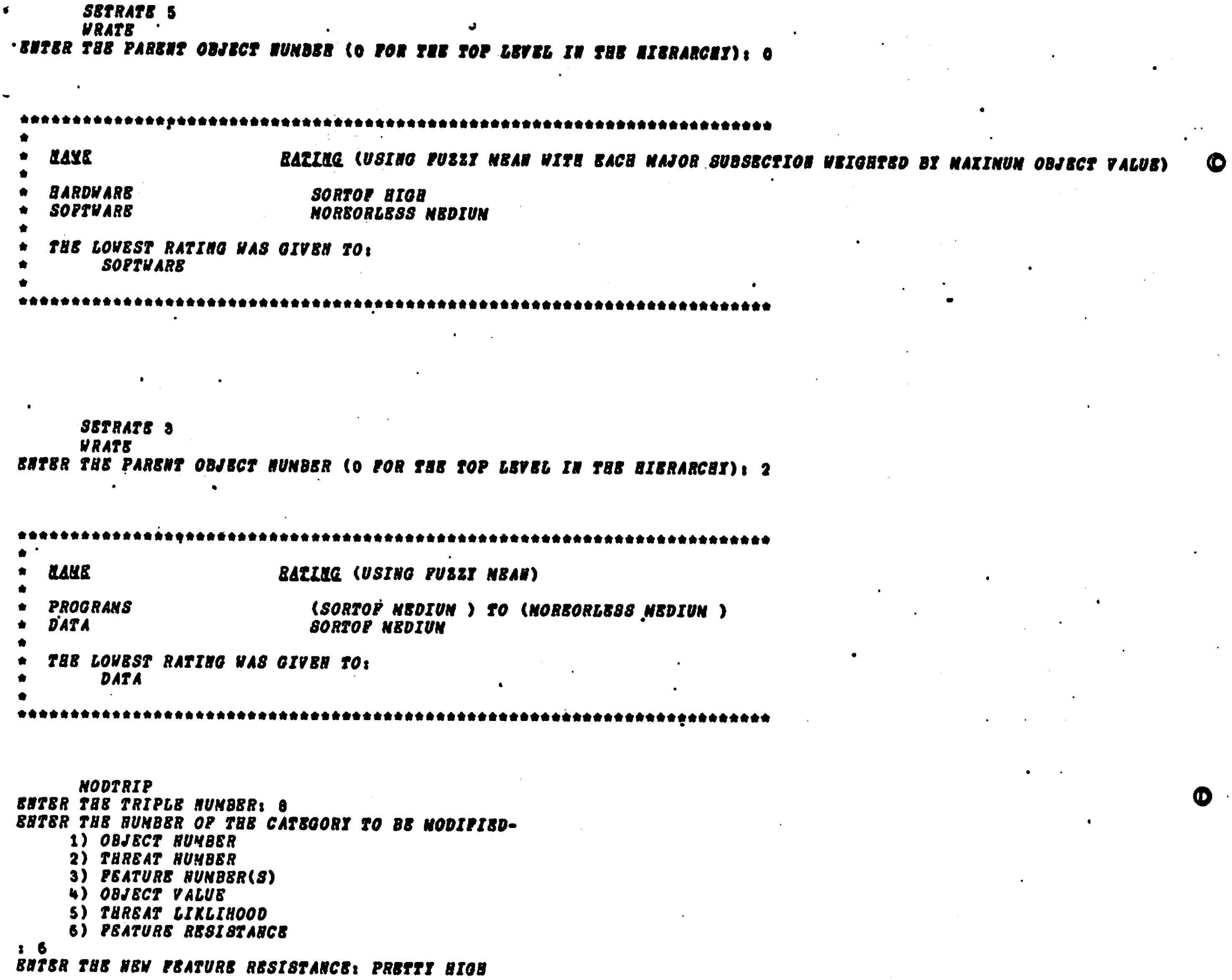
```
        RATESET
DO YOU WANT TO SEE A DESCRIPTION OF THE RATING FUNCTIONS? Y

    THE FOLLOWING RATING FUNCTIONS ARE AVAILABLE:
      1) WEAKEST LINK
      2) SELECTED WEAKEST LINK
      3) FUZZY MEAN
      4) FUZZY MEAN WEIGHTED BY VALUE
      5) FUZZY MEAN WITH EACH MAJOR SUBSECTION WEIGHTED BY MAXIMUM OBJECT VALUE

ENTER THE NUMBER OF THE RATING FUNCTION YOU WISH TO USE: 1

        OVERALLRATING


**********************************************************************
*
*  NAME                    RATING (USING WEAKEST LINK)
*
*  THE INSTALLATION           LOW
*
**********************************************************************


        WORSTSUBSECTION
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 0


**********************************************************************
*
*  NAME                    RATING (USING WEAKEST LINK)
*
*  HARDWARE                   PRETTY LOW
*  SOFTWARE                   LOW
*
*  THE LOWEST RATING WAS GIVEN TO:
*       SOFTWARE
*
**********************************************************************


        SETRATE 3
        INDIVIDUALRATING
ENTER THE NUMBER OF THE OBJECT TO BE RATED: 2


**********************************************************************
*
*  NAME                    RATING (USING FUZZY MEAN)
*
*  SOFTWARE                   SORTOF MEDIUM
*
**********************************************************************
```

Figure 4.1b Use of the security evaluation functions



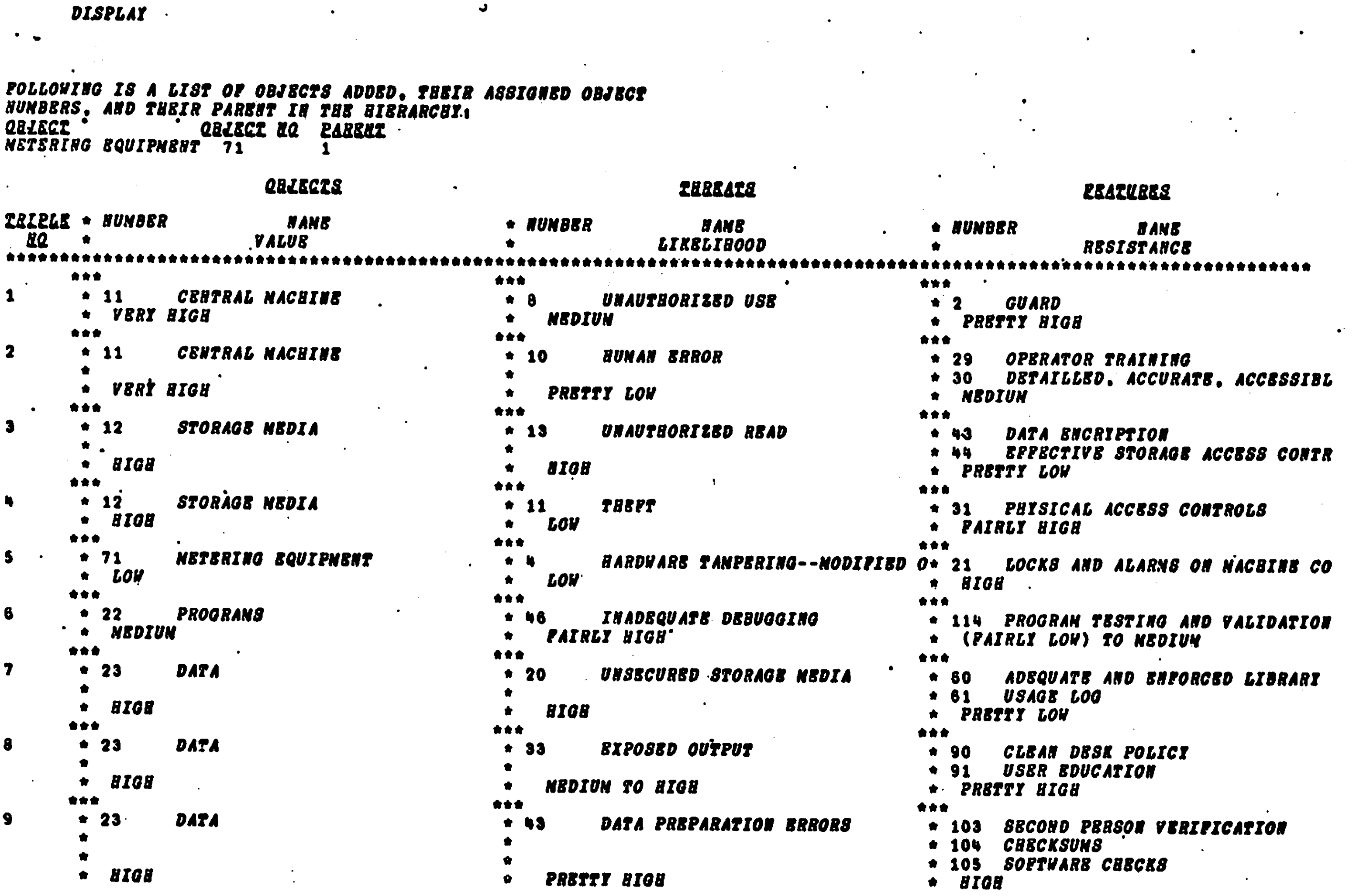
```
      SECTIONALRATING
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 0


**************************************************************************
*
*  NAME                     RATING (USING FUZZY MEAN)
*
*  HARDWARE                    ((SLIGHTLY LOWER ) THAN FAIRLY HIGH )AND (SLIGHTLY HIGHER ) THAN SORTOF HIGH
*  SOFTWARE                    SORTOF MEDIUM
*
**************************************************************************


      SETRATE 2
      WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 0
SPECIFY MINIMUM FOR HARDWARE : PRETTY HIGH
4 ELEMENT(S) USED
SPECIFY MINIMUM FOR SOFTWARE : PRETTY HIGH
3 ELEMENT(S) USED


**************************************************************************
*
*  NAME                     RATING (USING SELECTED WEAKEST LINK)
*
*  HARDWARE                    PRETTY LOW
*  SOFTWARE                    MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       HARDWARE
*
**************************************************************************


      SETRATE 4
      WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 0


**************************************************************************
*
*  NAME                     RATING (USING FUZZY MEAN WEIGHTED BY VALUE)
*
*  HARDWARE                    SORTOF HIGH
*  SOFTWARE                    MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       SOFTWARE
*
**************************************************************************
```

Figure 4.1c Continued use of the security evaluation functions



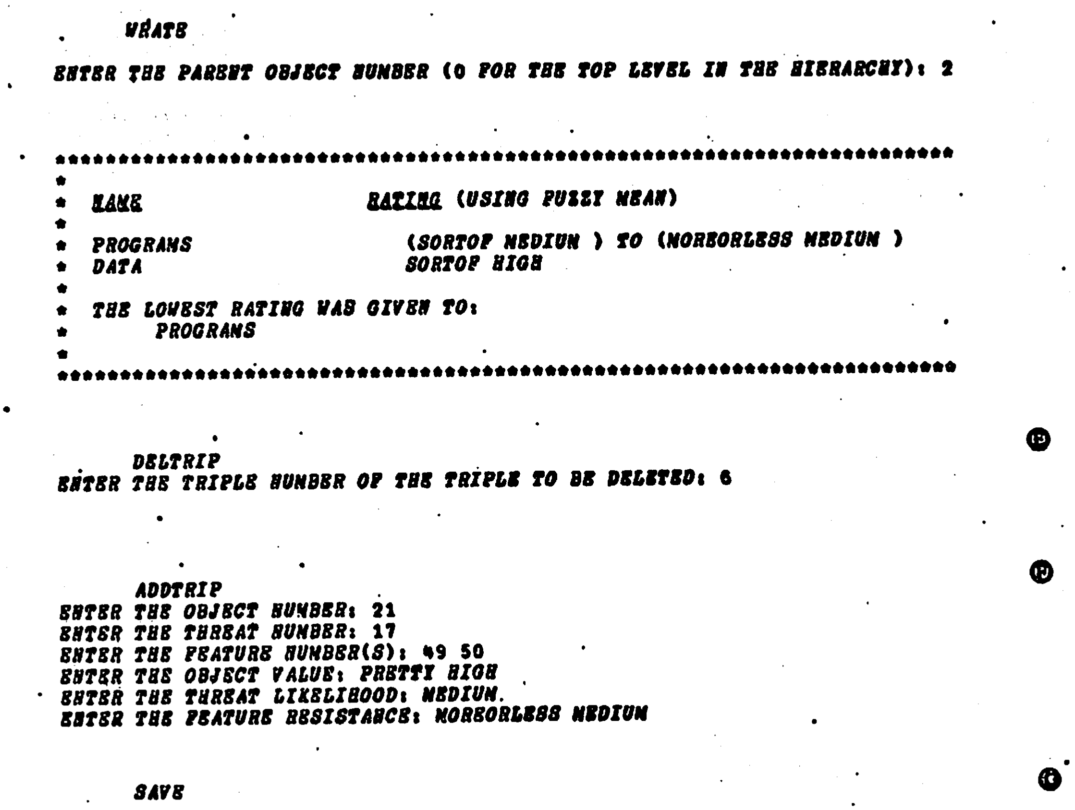
```
       SETRATE 5
       WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 0


**********************************************************************
*
*  NAME                    RATING (USING FUZZY MEAN WITH EACH MAJOR SUBSECTION WEIGHTED BY MAXIMUM OBJECT VALUE)
*
*  HARDWARE                   SORTOF HIGH
*  SOFTWARE                   MOREORLESS MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       SOFTWARE
*
**********************************************************************



       SETRATE 3
       WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 2


**********************************************************************
*
*  NAME                    RATING (USING FUZZY MEAN)
*
*  PROGRAMS                   (SORTOF MEDIUM ) TO (MOREORLESS MEDIUM )
*  DATA                       SORTOF MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       DATA
*
**********************************************************************


       MODTRIP
ENTER THE TRIPLE NUMBER: 8
ENTER THE NUMBER OF THE CATEGORY TO BE MODIFIED-
      1) OBJECT NUMBER
      2) THREAT NUMBER
      3) FEATURE NUMBER(S)
      4) OBJECT VALUE
      5) THREAT LIKLIHOOD
      6) FEATURE RESISTANCE
: 6
ENTER THE NEW FEATURE RESISTANCE: PRETTY HIGH
```

Figure 4.1d Use of the MODTRIP function and the security evaluation functions



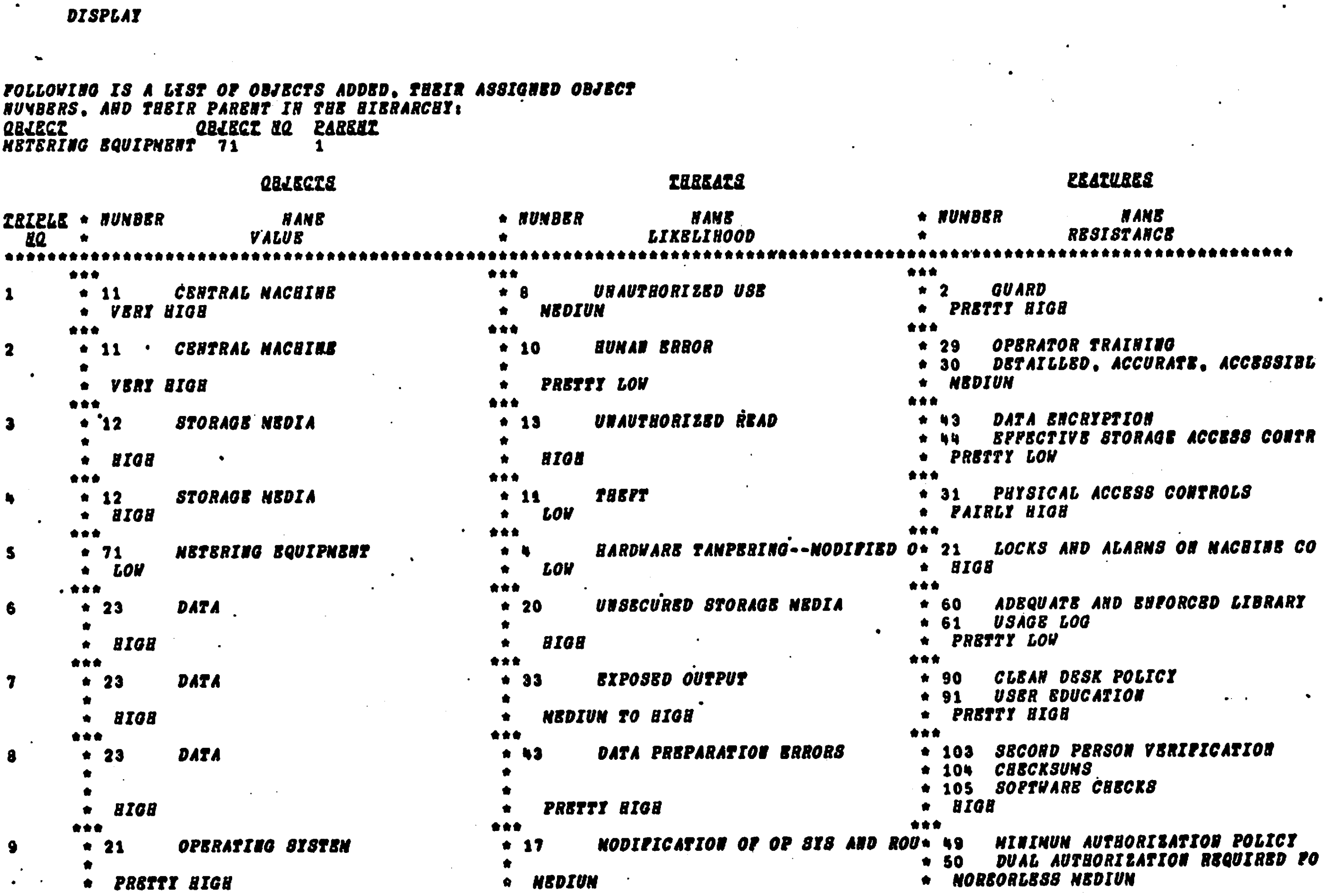
```
     DISPLAY


FOLLOWING IS A LIST OF OBJECTS ADDED, THEIR ASSIGNED OBJECT
NUMBERS, AND THEIR PARENT IN THE HIERARCHY:
OBJECT              OBJECT NO  PARENT
METERING EQUIPMENT  71         1

                         OBJECTS                                       THREATS                                          FEATURES

TRIPLE * NUMBER                NAME                * NUMBER           NAME                        * NUMBER            NAME
 NO    *                     VALUE                 *              LIKELIHOOD                      *                 RESISTANCE
*************************************************************************************************************************
      ***                                         ***                                            ***
1      * 11       CENTRAL MACHINE                  * 8       UNAUTHORIZED USE                     * 2    GUARD
       *  VERY HIGH                                *   MEDIUM                                     *  PRETTY HIGH
      ***                                         ***                                            ***
2      * 11       CENTRAL MACHINE                  * 10      HUMAN ERROR                          * 29   OPERATOR TRAINING
       *                                           *                                              * 30   DETAILLED, ACCURATE, ACCESSIBL
       *  VERY HIGH                                *   PRETTY LOW                                 *  MEDIUM
      ***                                         ***                                            ***
3      * 12       STORAGE MEDIA                    * 13      UNAUTHORIZED READ                    * 43   DATA ENCRIPTION
       *                                           *                                              * 44   EFFECTIVE STORAGE ACCESS CONTR
       *  HIGH                                     *   HIGH                                       *  PRETTY LOW
      ***                                         ***                                            ***
4      * 12       STORAGE MEDIA                    * 11      THEFT                                * 31   PHYSICAL ACCESS CONTROLS
       *  HIGH                                     *   LOW                                        *  FAIRLY HIGH
      ***                                         ***                                            ***
5      * 71       METERING EQUIPMENT               * 4       HARDWARE TAMPERING--MODIFIED O* 21   LOCKS AND ALARMS ON MACHINE CO
       *  LOW                                      *   LOW                                        *  HIGH
      ***                                         ***                                            ***
6      * 22       PROGRAMS                         * 46      INADEQUATE DEBUGGING                 * 114  PROGRAM TESTING AND VALIDATION
       *  MEDIUM                                   *   FAIRLY HIGH                                *  (FAIRLY LOW) TO MEDIUM
      ***                                         ***                                            ***
7      * 23       DATA                             * 20      UNSECURED STORAGE MEDIA              * 60   ADEQUATE AND ENFORCED LIBRARY
       *                                           *                                              * 61   USAGE LOG
       *  HIGH                                     *   HIGH                                       *  PRETTY LOW
      ***                                         ***                                            ***
8      * 23       DATA                             * 33      EXPOSED OUTPUT                       * 90   CLEAN DESK POLICY
       *                                           *                                              * 91   USER EDUCATION
       *  HIGH                                     *   MEDIUM TO HIGH                             *  PRETTY HIGH
      ***                                         ***                                            ***
9      * 23       DATA                             * 43      DATA PREPARATION ERRORS              * 103  SECOND PERSON VERIFICATION
       *                                           *                                              * 104  CHECKSUMS
       *                                           *                                              * 105  SOFTWARE CHECKS
       *  HIGH                                     *   PRETTY HIGH                                *  HIGH
```

Figure 4.1e Another data display



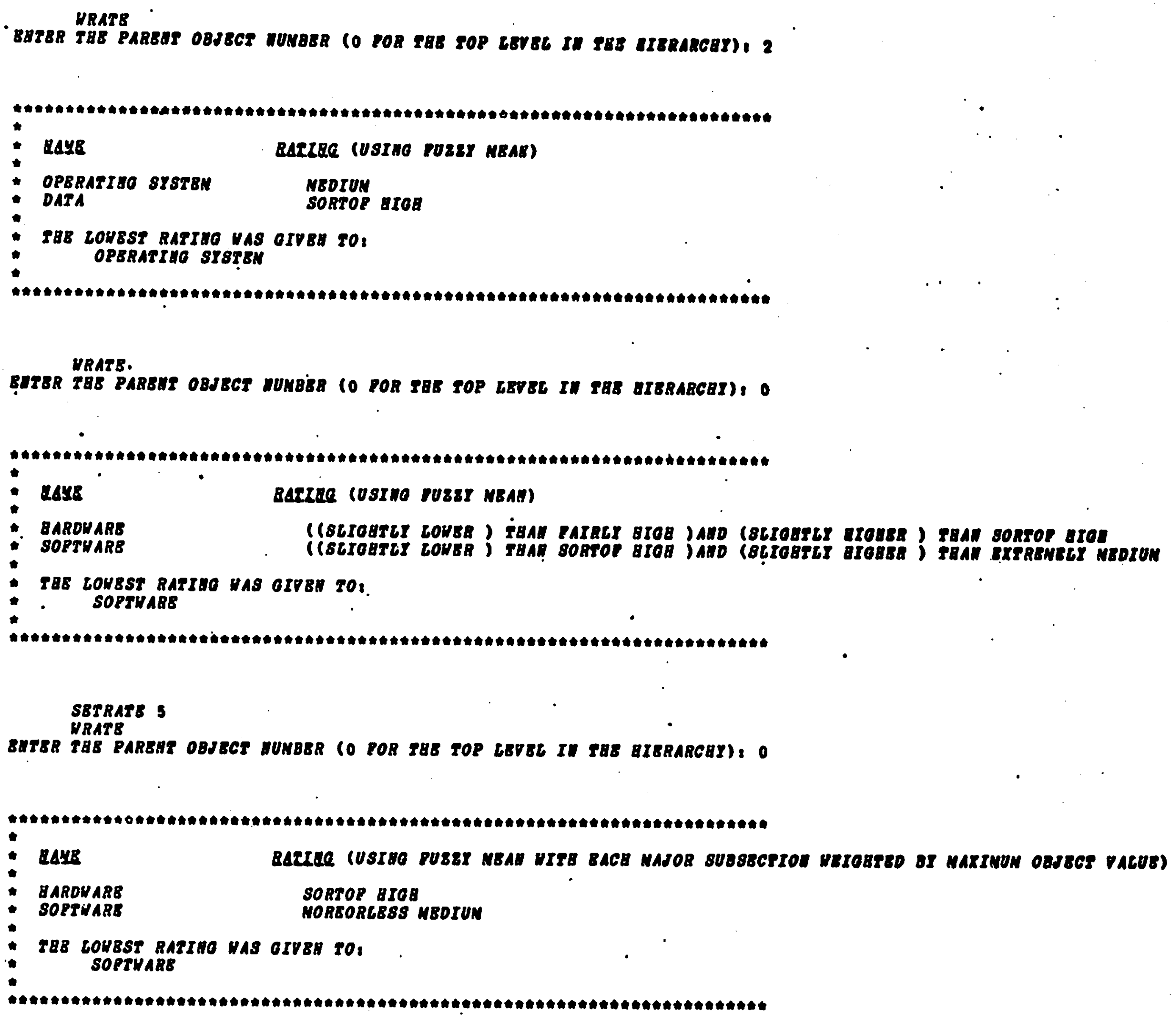
```
      WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 2


***************************************************************************
*
*  NAME                   RATING (USING FUZZY MEAN)
*
*  PROGRAMS                  (SORTOF MEDIUM ) TO (MOREORLESS MEDIUM )
*  DATA                      SORTOF HIGH
*
*  THE LOWEST RATING WAS GIVEN TO:
*       PROGRAMS
*
***************************************************************************



      DELTRIP
ENTER THE TRIPLE NUMBER OF THE TRIPLE TO BE DELETED: 6



      ADDTRIP
ENTER THE OBJECT NUMBER: 21
ENTER THE THREAT NUMBER: 17
ENTER THE FEATURE NUMBER(S): 49 50
ENTER THE OBJECT VALUE: PRETTY HIGH
ENTER THE THREAT LIKELIHOOD: MEDIUM.
ENTER THE FEATURE RESISTANCE: MOREORLESS MEDIUM


      SAVE
```

Figure 4.1f Use of the DELTRIP, ADDTRIP, and SAVE functions



```
DISPLAY


FOLLOWING IS A LIST OF OBJECTS ADDED, THEIR ASSIGNED OBJECT
NUMBERS, AND THEIR PARENT IN THE HIERARCHY:
OBJECT            OBJECT NO  PARENT
METERING EQUIPMENT  71        1
                        OBJECTS                               THREATS                              FEATURES

TRIPLE * NUMBER           NAME                * NUMBER          NAME                 * NUMBER           NAME
 NO    *               VALUE                  *             LIKELIHOOD               *             RESISTANCE
************************************************************************************************************************
      ***                                    ***                                    ***
1      * 11     CENTRAL MACHINE               * 8      UNAUTHORIZED USE              * 2    GUARD
       *  VERY HIGH                           *   MEDIUM                             *  PRETTY HIGH
      ***                                    ***                                    ***
2      * 11     CENTRAL MACHINE               * 10     HUMAN ERROR                   * 29   OPERATOR TRAINING
       *                                      *                                      * 30   DETAILLED, ACCURATE, ACCESSIBL
       *  VERY HIGH                           *   PRETTY LOW                         *  MEDIUM
      ***                                    ***                                    ***
3      * 12     STORAGE MEDIA                 * 13     UNAUTHORIZED READ             * 43   DATA ENCRYPTION
       *                                      *                                      * 44   EFFECTIVE STORAGE ACCESS CONTR
       *  HIGH                                *   HIGH                               *  PRETTY LOW
      ***                                    ***                                    ***
4      * 12     STORAGE MEDIA                 * 11     THEFT                         * 31   PHYSICAL ACCESS CONTROLS
       *  HIGH                                *   LOW                                *  FAIRLY HIGH
      ***                                    ***                                    ***
5      * 71     METERING EQUIPMENT            * 4      HARDWARE TAMPERING--MODIFIED O* 21   LOCKS AND ALARMS ON MACHINE CO
       *  LOW                                 *   LOW                                *  HIGH
      ***                                    ***                                    ***
6      * 23     DATA                          * 20     UNSECURED STORAGE MEDIA       * 60   ADEQUATE AND ENFORCED LIBRARY
       *                                      *                                      * 61   USAGE LOG
       *  HIGH                                *   HIGH                               *  PRETTY LOW
      ***                                    ***                                    ***
7      * 23     DATA                          * 33     EXPOSED OUTPUT                * 90   CLEAN DESK POLICY
       *                                      *                                      * 91   USER EDUCATION
       *  HIGH                                *   MEDIUM TO HIGH                     *  PRETTY HIGH
      ***                                    ***                                    ***
8      * 23     DATA                          * 43     DATA PREPARATION ERRORS       * 103  SECOND PERSON VERIFICATION
       *                                      *                                      * 104  CHECKSUMS
       *                                      *                                      * 105  SOFTWARE CHECKS
       *  HIGH                                *   PRETTY HIGH                        *  HIGH
      ***                                    ***                                    ***
9      * 21     OPERATING SYSTEM              * 17     MODIFICATION OF OP SYS AND ROU* 49   MINIMUM AUTHORIZATION POLICY
       *                                      *                                      * 50   DUAL AUTHORIZATION REQUIRED FO
       *  PRETTY HIGH                         *   MEDIUM                             *  MOREORLESS MEDIUM
```

Figure 4.1g Another data display



```
        WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 2


**********************************************************************
*
*  NAME                     RATING (USING FUZZY MEAN)
*
*  OPERATING SYSTEM            MEDIUM
*  DATA                        SORTOF HIGH
*
*  THE LOWEST RATING WAS GIVEN TO:
*       OPERATING SYSTEM
*
**********************************************************************


        WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 0


**********************************************************************
*
*  NAME                     RATING (USING FUZZY MEAN)
*
*  HARDWARE                    ((SLIGHTLY LOWER ) THAN FAIRLY HIGH )AND (SLIGHTLY HIGHER ) THAN SORTOF HIGH
*  SOFTWARE                    ((SLIGHTLY LOWER ) THAN SORTOF HIGH )AND (SLIGHTLY HIGHER ) THAN EXTREMELY MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       SOFTWARE
*
**********************************************************************


        SETRATE 5
        WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 0


**********************************************************************
*
*  NAME                     RATING (USING FUZZY MEAN WITH EACH MAJOR SUBSECTION WEIGHTED BY MAXIMUM OBJECT VALUE)
*
*  HARDWARE                    SORTOF HIGH
*  SOFTWARE                    MOREORLESS MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       SOFTWARE
*
**********************************************************************
```

Figure 4.1h Continued use of the security evaluation functions

The following security evaluation functions are available. To invoke one type either the full name or the shortened form.

OVERALLRATING (also ORATE)--This function returns a security rating for the entire installation (refer to point ③, figure 4.1). That is, it rates the entire set of triples.

INDIVIDUALRATING (also IRATE)--This function returns a security rating for a specified subsection of the installation ⑦. Only triples for that subsection, including offspring, are considered. For example, for an individual subsection rating of the central machine, the evaluation system would consider triples specified for the central machine and each of its offspring: the CPU, main memory, I/O devices, and the operator's console (this section of the hierarchy was illustrated in figure 1.1).

SECTIONALRATING (also SRATE)--Prompting the user for either the top level of the hierarchy or one of the subsections, this function returns an individual rating for each subsection at the next lower level ⑨. For example, if the top level of the hierarchy was specified, SECTIONALRATING would return a security rating for each of hardware, software, the computer center, personnel, documentation, and the backup system.

WORSTSUBSECTION (also WRATE)--this performs the same function as SECTIONALRATING, with the additional feature that it highlights the subsection receiving the lowest rating ⑤.

4.2 The Scoring Options

In addition to choosing which of the above analysis functions to use, the user must also choose among four scoring methods of producing a security rating for a given set of triples. Following are the five options:

Weakest link--this will look for the weakest feature resistance and return that as the security rating ④. The philosophy here is that the system is only as secure as its weakest link.

Selected weakest link--this produces a weakest link rating based on those triples which satisfy the condition that either their object value or the threat likelihood is greater than a user specified minimum Ⓐ. The idea here is that one would only want to consider triples where the object is of at least a certain value or the threat is of at least a certain likelihood.

Fuzzy mean--this performs a fuzzy mean [1] on the feature resistances and returns the result as the rating ⑧. The theory here is that a system's security is the mean of the security of its components.

Weighted fuzzy mean--this performs a fuzzy mean on the feature resistance weighted by the greater of the object value and threat likelihood for each triple Ⓑ. The theory is that of the fuzzy mean, with the additional assumption that the more valuable objects and those with more likely threats should receive greater weight in the security rating.

Fuzzy mean with each major subsection weighted by maximum object value-- for each major subsection of the object specified, this finds the fuzzy mean of the resistances. It then weights these fuzzy means by the maximum object value found in the triples for each major subsection and averages these weighted means Ⓒ. In other words, it finds the fuzzy means for each major subsection and weights them by their respective maximum object value. The theory is similar to that of the weighted fuzzy mean, but with the assumption that the major subsections should be weighted be their relative values, irrespective of the number of triples they each have.

To specify a rating function, the user types RATESET ②, and a prompt is printed asking for the choice. Alternatively, the user may type SETRATE ⑥ followed by the number of his choice (try RATESET once to see the choice numbers). Once the user specifies a rating function, it stays in effect for all of the evaluation functions until it is respecified.

4.3 System Functions

Following are the system utilities available to the user.

DISPLAY--this formats and prints the triples information, including object name, number, and value, threat name, number, and likelihood, and feature resistance ①.

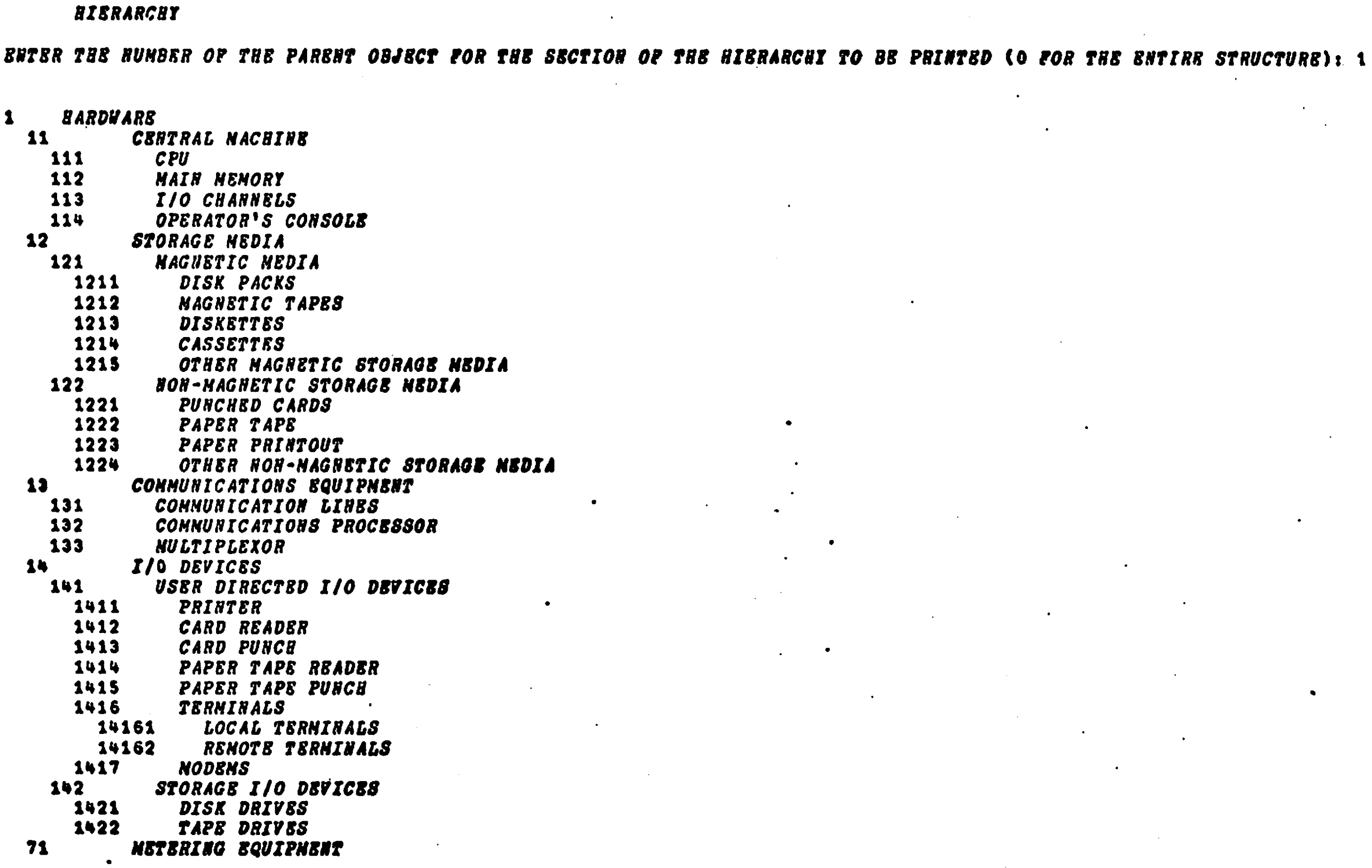
ADDTRIP--this function allows the user to add individual triples quickly (see also SAVE) Ⓕ.

DELTRIP--this function deletes an existing triple (see also SAVE) Ⓔ.

MODTRIP--this function allows the user to modify existing triples (see also SAVE) Ⓓ.

SAVE--this function saves all of the user's data in the user's workspace Ⓖ. This should be executed after changes have been made.

HIERARCHY--this prints all or part of the object hierarchy for the user's installation. Figure 4.2 illustrates the use of the HIERARCHY function with the data input in figure 3.2.



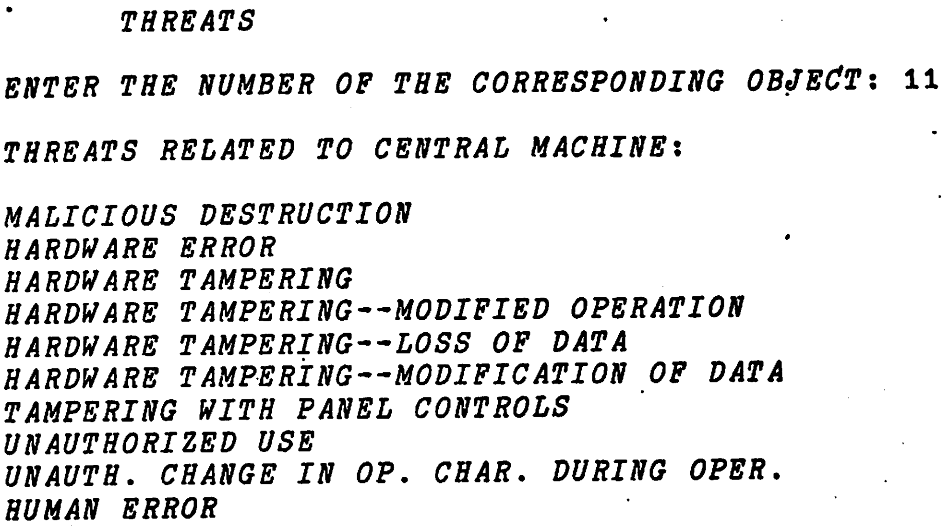
```
     HIERARCHY

ENTER THE NUMBER OF THE PARENT OBJECT FOR THE SECTION OF THE HIERARCHY TO BE PRINTED (0 FOR THE ENTIRE STRUCTURE): 1

1     HARDWARE
  11        CENTRAL MACHINE
    111       CPU
    112       MAIN MEMORY
    113       I/O CHANNELS
    114       OPERATOR'S CONSOLE
  12        STORAGE MEDIA
    121       MAGNETIC MEDIA
      1211      DISK PACKS
      1212      MAGNETIC TAPES
      1213      DISKETTES
      1214      CASSETTES
      1215      OTHER MAGNETIC STORAGE MEDIA
    122       NON-MAGNETIC STORAGE MEDIA
      1221      PUNCHED CARDS
      1222      PAPER TAPE
      1223      PAPER PRINTOUT
      1224      OTHER NON-MAGNETIC STORAGE MEDIA
  13        COMMUNICATIONS EQUIPMENT
    131       COMMUNICATION LINES
    132       COMMUNICATIONS PROCESSOR
    133       MULTIPLEXOR
  14        I/O DEVICES
    141       USER DIRECTED I/O DEVICES
      1411      PRINTER
      1412      CARD READER
      1413      CARD PUNCH
      1414      PAPER TAPE READER
      1415      PAPER TAPE PUNCH
      1416      TERMINALS
        14161     LOCAL TERMINALS
        14162     REMOTE TERMINALS
      1417      MODEMS
    142       STORAGE I/O DEVICES
      1421      DISK DRIVES
      1422      TAPE DRIVES
  71        METERING EQUIPMENT
```

Figure 4.2 Use of the HIERARCHY function

4.4 Information Facilities

Following are the informational facilities available.

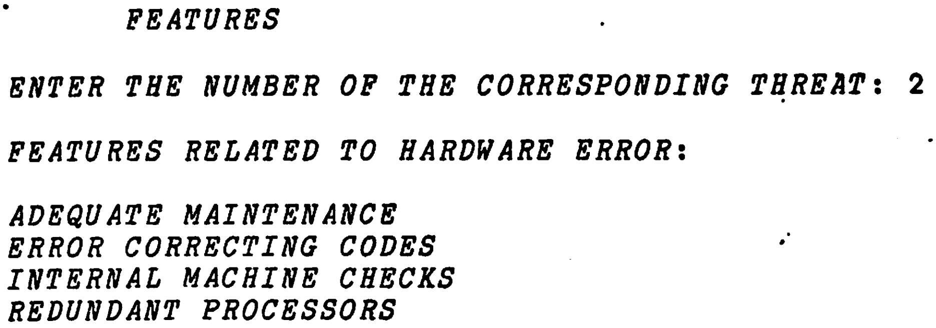
THREATS--this prints out common threats for a given object in the hierarchy. An example of this is shown in figure 4.3.



```
        THREATS

ENTER THE NUMBER OF THE CORRESPONDING OBJECT: 11

THREATS RELATED TO CENTRAL MACHINE:

MALICIOUS DESTRUCTION
HARDWARE ERROR
HARDWARE TAMPERING
HARDWARE TAMPERING--MODIFIED OPERATION
HARDWARE TAMPERING--LOSS OF DATA
HARDWARE TAMPERING--MODIFICATION OF DATA
TAMPERING WITH PANEL CONTROLS
UNAUTHORIZED USE
UNAUTH. CHANGE IN OP. CHAR. DURING OPER.
HUMAN ERROR
```

Figure 4.3 Use of the THREATS function

FEATURES--this prints out common security features for a given threat in the threat listing. An example of this is shown in figure 4.4.



```
        FEATURES

ENTER THE NUMBER OF THE CORRESPONDING THREAT: 2

FEATURES RELATED TO HARDWARE ERROR:

ADEQUATE MAINTENANCE
ERROR CORRECTING CODES
INTERNAL MACHINE CHECKS
REDUNDANT PROCESSORS
```

Figure 4.4 Use of the FEATURES function

BIBLIOGRAPHY

[1] "SECURATE: A Security Evaluation and Analysis System Using Fuzzy Metrics", Eric H. Michelman and Lance J. Hoffman, Memorandum No. UCB/ERL M77/36, Electronics Research Laboratory, College of Engineering, University of California, Berkeley, July 1977.

[2] "Fuzzy Ratings for Computer Security Evaluation", Don Clements, Memorandum No. UCB/ERL M77/41, Electronics Research Laboratory, College of Engineering, University of California, Berkeley, June 1977.

[3] "A Practical Framework for Computer Installation Security", Eric H. Michelman, Memorandum No. UCB/ERL M77/4, Electronics Research Laboratory, College of Engineering, University of California, Berkeley, June 1977.

[4] "The Concept of the Lingistic Variable and its Application to Approximate Reasoning", L. A. Zadeh, Memorandum No. ERL-M411, Electronics Research Laboratory, College of Engineering, University of California, Berkeley, October 1973.

Appendix A

The Object Hierarchy and

Threats, Features, and Flaws Listings

In addition to objects, threats, and features, another category is introduced, that of flaws. Flaws are defined as characteristics of a computing system which enhance the likelihood of a threat succeeding in compromising an object. While flaws are not considered by the system, they were developed as a user convenience. Their purpose is to map what a user may view as threats into threats as viewed by the model. A simple example of this would be leaving confidential material exposed. It would be reasonable to view this as a threat to security, however Clements' security model takes the position that the security threat would be an unauthorized person viewing the exposed material. In practice, though, the user should feel free to specify whatever he feels most comfortable with.

The Object Hierarchy

1. Hardware
2. Software
3. The Computer Center
4. Personnel
5. Documentation
6. Backup system

1. Hardware

- 1.1 Central machine
  - 1.1.1 CPU
  - 1.1.2 Main memory
  - 1.1.3 I/O channels
  - 1.1.4 Operator's console
- 1.2 Storage medium
  - 1.2.1 Magnetic media
    - 1.2.1.1 Disk packs
    - 1.2.1.2 Magnetic tapes
    - 1.2.1.3 Diskettes (floppies)
    - 1.2.1.4 Cassettes
    - 1.2.1.5 Other
  - 1.2.2 Non-magnetic media
    - 1.2.2.1 Punched cards
    - 1.2.2.2 Paper tape
    - 1.2.2.3 Paper printout
    - 1.2.2.4 Other
- 1.3 Communications equipment
  - 1.3.1 Communications lines
  - 1.3.2 Communications processor
  - 1.3.3 Multiplexor
- 1.4 I/O devices
  - 1.4.1 User directed I/O devices
    - 1.4.1.1 Printer
    - 1.4.1.2 Card reader
    - 1.4.1.3 Card punch
    - 1.4.1.4 Paper tape reader
    - 1.4.1.5 Paper tape punch
    - 1.4.1.6 Terminals
      - 1.4.1.6.1 Local terminals
      - 1.4.1.6.2 Remote terminals
    - 1.4.1.7 Modems
  - 1.4.2 Storage I/O devices
    - 1.4.2.1 Disk drives
    - 1.4.2.2 Tape drives

2. Software

2.1 Operating system

2.2 Programs

2.2.1 Applications

2.2.1.1 Source

2.2.1.2 Non-source

2.2.2 Contract programs and packages

2.2.3 System utilities

2.2.4 Test programs

2.3 Data

2.3.1 Personal data

2.3.1.1 Payroll

2.3.1.2 Personnel

2.3.1.3 Other personal data (Privacy Act of 1974, §3(a)(4))

2.3.2 Institution data

2.3.2.1 Marketing

2.3.2.2 Financial

2.3.2.3 Operations

2.3.2.4 Planning

2.3.2.5 Other

3. The Computer Center

- 3.1 Resource supply systems
  - 3.1.1 Air conditioning
  - 3.1.2 Power
  - 3.1.3 Water
  - 3.1.4 Lighting
- 3.2 Building
  - 3.2.1 Structure
  - 3.2.2 Computer operations
    - 3.2.2.1 Computer room
    - 3.2.2.2 Data reception
    - 3.2.2.3 Tape and disc library
    - 3.2.2.4 CE room
    - 3.2.2.5 Data preparation area
    - 3.2.2.6 Physical plant room
    - 3.2.2.7 Stationery storage
- 3.3 Waste materials
  - 3.3.1 Paper
  - 3.3.2 Ribbons
  - 3.3.3 Magnetic materials

4. Personnel

- 4.1 Computer personnel
  - 4.1.1 Supervisory personnel
  - 4.1.2 Systems analysts
  - 4.1.3 Programmers
    - 4.1.3.1 Applications programmers
    - 4.1.3.2 Systems programmers
  - 4.1.4 Operators
    - 4.1.4.1 First shift
    - 4.1.4.2 Second and third shifts
  - 4.1.5 Librarians
  - 4.1.6 Temporary employees and consultants
  - 4.1.7 Maintenance personnel
  - 4.1.8 System evaluators and auditors
  - 4.1.9 Clerical personnel
- 4.2 Building personnel
  - 4.2.1 Janitors
  - 4.2.2 Watchmen
- 4.3 Institution executives
- 4.4 Other personnel

5. Documentation

- 5.1 Software documentation
  - 5.1.1 File
  - 5.1.2 Program
  - 5.1.3 JCL
  - 5.1.4 System
- 5.2 Hardware documentation
- 5.3 Operations
  - 5.3.1 Schedules
  - 5.3.2 Operations guidelines and manuals
  - 5.3.3 Audit documents

6. Backup system

6.1 Hardware

6.1.1 Replacement for equipment detailed in section 1

6.1.2 Replacement time

6.2 Backup for software detailed in section 2

6.3 The Computer Center

6.3.1 Electric power generation

6.3.2 Generator fuel supply

6.3.3 Water supply

6.4 Auxiliary personnel

6.5 Documentation, operational procedures

6.5.1 Vital records

6.5.2 Priority run schedules

6.5.3 Backup for documentation in section 5

Threats and Flaws

The structure of the threats list is based on the object hierarchy, which is used as an outline. Threats are listed after the objects they refer to, the objects being specified by name and number from the object hierarchy. A threat listed after a non-terminal node of the object hierarchy refers to all objects decending from that node. The threat numbers are listed down the left side, along side the threats they refer to.

The numbers of relevant flaws are listed after each threat. The flaw numbers are preceded by an "F" and are ordered sequentially within each of the six main object/threat categories. The flaws themselves are listed along with their corresponding numbers after threat listings for each of the six main categories.

1. Hardware

1.1 Central machine

1) Malicious destruction - F1.1

2) Hardware error - F1.4

3) Hardware tampering - F1.1, F1.4, F1.5

4) modified operation

5) loss of data

6) modification of data

7) Tampering with panel controls

8) Unauthorized use - F1.2

9) Unauthorized change in operating characteristics during operation - F1.2

10) Human error - F1.6, F1.7

1.2 Storage media

11) Theft - F1.3

12) Unauthorized modification - F1.3

13) Unauthorized read - F1.3

1.3 Communications equipment

14) <same threats as 1.1 Central machine>

1.4 I/O devices

15) <same threats as 1.1 Central machine>

Hardware Flaws

F1.1 Inadequate plant security

F1.2 Lack of status indicators

F1.3 Inadequate storage library security

- authorization
- guard
- labeling
- diligence in keeping materials stored properly

F1.4 Lack of machine checks, hardware and software

F1.5 Unsupervised or unauthenticated CE activity

F1.6 Operator ignorance

F1.7 Misleading documentation, incomplete or inadequate

2. Software

16) A. Unauthorized access: R/W/E - F2.1, F2.2

17) Modification of operating system and system routines

18) Inadequate controls on I/O facilities - F2.3, F2.4

19) Password compromise - F2.5, F2.6, F2.7, F2.8

20) Unsecured storage medium - F2.9, F2.10, F2.11, F2.12

21) Access outside of allocated memory - F2.13, F2.14, F2.15

22) Modification of stored state vector - F2.16

23) Unauthorized CE activity

24) Line tapping and spoofing

25) Erroneous or inadequate usage of protection facilities - F2.17, F2.18, F2.19

26) B. Unauthorized access: read

27) Extra copies of output printed

28) duplicates printed

29) printing restarted before end

30) Use of erroneous distribution labels

31) Use of erroneous distribution lists

32) Theft of mail

33) Exposed output - F2.20, F2.21

34) in user possession

35) within distribution system

36) at operator's console

37) work in progress

38) Unauthorized reading of terminal buffers

39) Indirect exposure of output - F2.22, F2.23

40) C. Unauthorized access: write

41) Modification or spoof of mail transactions

42) Unauthorized modification of data during preparation - F2.24

43) Data preparation errors - F2.24

44) Modification of original written data input - F2.25

2.1 Operating system

45) Defective implementation - F2.26, F2.27, F2.28, F2.29, F2.30, F2.31, F2.32

2.2 Programs

46) Inadequate debugging

47) Incomplete operation specifications

48) Inadequate or erroneous error handling

49) Exposure following abnormal end

5Ø) Improper operation

2.2.2 Contract programs and packages

51) Dishonest programs

2.2.4 Test programs

52) Unexpected alteration of real data

Software Flaws

F2.1 Faulty access control mechanism

F2.2 Non-functional protected state mechanism

F2.3 Ability to use self-modifying I/O code

F2.4 Ability to write file into other user's catalog

F2.5 Printout of password at terminal

F2.6 Exposed input on spooling facility

F2.7 Use of user selected password

F2.8 Storage of password in unencrypted form

F2.9 Inadequate physical access controls

F2.10 Inadequate operator procedure

F2.11 Ability to spoof operator

F2.12 Improper labeling

F2.13 Inadequate base/bounds checking

F2.14 Unprotected storage after system crash

F2.15 Unprotected storage during system initialization

F2.16 State vector stored in user storage

F2.17 User interface of protection system too complex

F2.18 Inaccurate documentation

F2.19 Incomplete documentation

F2.20 Materials left exposed during emergency

F2.21 Output not checked for proper content

F2.22 Sensitive jobs printed with new ribbon

F2.23 Exposed waste materials

F2.24 Inadequate total and edit checks

F2.25 Inadequate control of hard copy input data

F2.26 Excessive complexity

F2.27 Non-detected bugs (inadequate testing)

F2.28 Improper design specifications

F2.29 Access control based on checking for lack of permission

F2.30 Effectiveness of protection system based on ignorance

F2.31 Overprivileged system modules

F2.32 Lack of violation recording and review

3. The Computer Center

3.1 Resource supply systems

53) Natural calamities

54) Fire

55) Flood

56) Earthquake

57) Manmade disasters

58) Smoke

59) Rioting

60) Bombing

61) Vandalism

62) Fate (chance events)

63) Equipment breakdown

64) Shutdown of building facilities

3.1.2 Power

65) Blackout

66) Fluctuations

67) Grounding problems

3.1.3 Water

68) Disruption

69) Contamination

70) Temperature variations

3.1.4 Lighting

71) Blackout

3.2 The Building

72) Natural calamities

73) Fire

74) Flood

75) Earthquake

76) Manmade disasters

77) Smoke

78) Rioting

79) Bombing

80) Vandalism

3.2.2 Computer operations area

81) Shocks and vibrations

82) Communications breakdown

83) Illegal entry and burglary

3.2.2.1 Computer room

84) Magnets

85) Electromagnetic radiation, to and from

3.2.2.2 Data reception

86) Unauthorized intruders

3.2.2.3 Tape and disk library

87) Magnets

3.2.2.6 Physical plant room

88) Sabotage

3.3 Waste materials

89) Unauthorized reading

90) Theft

4. Personnel

91) Bribery - F4.1

92) Dissatisfaction or malice - F4.1, F4.2

93) Towards the institution

94) Towards management

95) Towards other workers

96) Towards others (possibly unknown)

97) Greed - F4.1, F4.2

98) Competitor encouraged

99) Entrepreneurial tendencies

100) Incompetence - F4.1

101) Coercion - F4.1, F4.2

102) Competitor plants (industrial espionage)

103) Carelessness - F4.1

Personnel Flaws

F4.1 Personal instability

F4.2 Job insecurity

5. Documentation

104) Loss - F5.1, F5.2

105) Thievery - F5.1, F5.2

106) Unauthorized viewing - F5.1, F5.2

107) Unauthorized modification - F5.1, F5.2

Documentation Flaws

F5.1 Inadequate signout procedures

F5.2 Documentation left unsecured

6. Backup system

108) Limited or no accessibility - F6.1, F6.2, F6.3, F6.4, F6.5

6.1 Hardware

109) Incompatibility with other equipment in use

110) Ignorance of operation

111) <additionally, same considerations as section 1, Hardware threats>

6.2 Software

112) Not up to date

113) Incompatible system components

114) Ignorance of use

115) Lack of necessary data

116) <additionally, same considerations as section 2, Software threats>

6.3 The Computer Center

117) Malfunctioning power generation system

118) Shortage of generator fuel

119) Shortage of operation materials

120) <additionally, same considerations as section 3, Computer Center threats>

6.4 Personnel

121) Lack of transportation to backup site

122) Lack of communication

6.5 Documentation, operational procedures

123) Inadequate communications facilities

124) Incompatible run procedures

125) Inadequate office, other operational facilities

126) Unplanned emergency run schedules

127) Inadequate personnel direction

128) Confusion during disaster - F6.6

129) <additionally, same considerations as section 5, Documentation threats>

Backup System Flaws

F6.1 Excessive time involved in traveling to backup installation

F6.2 Excessive distance involved in traveling to backup installation

F6.3 Excessive cost involved in transportation to backup installation

F6.4 Ignorance about how to get at backup (real-time)

F6.5 Non-existence of all or part of backup

F6.6 Lack of simulated disaster tests

```
PRINTFEATURES


FEATURE NO  THREAT NOS      FEATURE NAME

   1          1             PHYSICAL SECURITY
   2                             GUARD
   3                             ID CARD DOOR
   4                             PROPER LOCATION OF CENTER
   5                             SECURE DOOR AND WINDOW LOCKS
   6                             PERSONAL SEARCHES
   7                             TWO OPERATOR SYSTEM
   8                             ENTRANCE LOG
   9                             OUTSIDE LIGHTING
  10                             FENCE
  11                             ALARM SYSTEM
  12                             CLOSED CIRCUIT TV
  13                             ID BADGES
  14                             SECURE DOORS AND WINDOWS

  15          2             ADEQUATE MAINTENANCE
  16                        ERROR CORRECTING CODES
  17                        INTERNAL MACHINE CHECKS
  18                        REDUNDANT PROCESSORS

  19          3 4 5 6       <THE SAME FEATURES AS THREAT NO. 1>
  20                        SUPERVISION AND AUTHENTICATION OF CE'S
  21                        LOCKS AND ALARMS ON MACHINE COVERS

  22          7             <THE SAME FEATURES AS THREAT NO. 1>

  23          8             AUTOMATIC LOG
  24                        LOCKS ON CONTROLS
  25                        <ADDITIONALLY, THE SAME FEATURES AS THREAT NO. 1>

  26          9             STATUS INDICATORS
  27                        AUTOMATIC LOG

  28          10            PROPER LABELLING
  29                        OPERATOR TRAINING
  30                        DETAILLED, ACCURATE, ACCESSIBLE DOCUMENTATION

  31          11            PHYSICAL ACCESS CONTROLS
  32                             PACKAGE AND BRIEFCASE INSPECTION
  33                             GATE-PASS SYSTEM
  34                             SECURE LIBRARY FACILITY
  35                             PROPER LABELLING

  36          12            CONTROL CHECKS
  37                             CHECKSUM ON DATA
  38                             EFFECTIVE STORAGE ACCESS CONTROLS
  39                             HEADER CHECKING
  40                             PREVENTIVE MEASURES
  41                             WRITE-INHIBIT SWITCHES
  42                             RING OUT FOR TAPES

  43          13            DATA ENCRYPTION
  44                        EFFECTIVE STORAGE ACCESS CONTROLS

  45          14 15         <THE SAME FEATURES AS THREATS 1-13>

  46          16            EFFECTIVE AUTHORIZATION AND ACCESS CONTROL MECHANISM
```

46	16	EFFECTIVE AUTHORIZATION AND ACCESS CONTROL MECHANISM
47		MINIMUM AUTHORIZATION POLICY
48	17	EFFECTIVE AUTHORIZATION AND ACCESS CONTROL MECHANISM
49		MINIMUM AUTHORIZATION POLICY
50		DUAL AUTHORIZATION REQUIRED FOR CHANGES
51		SUPER USER AUTHORIZATION REQUIRED FOR CHANGES
52		LOG OF ATTEMPTED VIOLATIONS
53	18	SELF-MODIFYING I/O ROUTINES NOT ALLOWED
54	19	DIRECTION IN PASSWORD CHOICE
55		STORE IN ENCRYPTED FORM
56		AUTOMATIC DELAY AFTER INVALID LOGIN ATTEMPT
57		ENCRYPTED TRANSMISSIONS TO TERMINALS
58		USE OF INTERACTIVE AUTHENTICATION PROCEDURE
59	20	ADEQUATE ACCESS CONTROLS
60		ADEQUATE AND ENFORCED LIBRARY FACILITY
61		USAGE LOG
62		PROPER LABELLING
63	21	PROPER SYSTEM DESIGN
64		EFFECTIVE AUTHORIZATION AND ACCESS CONTROL MECHANISM
65		ADEQUATE I/O CONTROLS
66		PROTECTION OF STATE VECTOR
67	22	STORAGE IN PROTECTED STORAGE
68	23	ADMINISTRATIVE CONTROLS
69		HUMAN VERIFICATION
70		SUPERVISION
71		LIMITED CE ACCESS
72	24	ENCRYPTION
73	25	EFFECTIVE HUMAN ENGINEERING
74		CLEAR, EASY TO USE PROTECTION FACILITIES
75		ADEQUATE DOCUMENTATION
76		USER EDUCATION
77	26	<SEE FEATURES FOR THREATS 27-39>
78	27	PRINT LOG
79		SECURITY CONSCIOUS I/O ROUTINES
80	28	PRINT LOG
81	29	PRINT LOG
82		SECURITY CONSCIOUS I/O ROUTINES
83	30 31	CAREFUL ADMINISTRATIVE PROCEDURES
84	32	CAREFUL ADMINISTRATIVE PROCEDURES
85		IMPORTANT MAIL SENT REGISTERED OR BY COURIER
86		DELIVERY CONFIRMATION
87	33	TRACE LOG OF SENSITIVE OUTPUT
88		LIBRARY FACILITY FOR SENSITIVE OUTPUT
89		<SEE ALSO FEATURES FOR THREATS 34-37>
90	34	CLEAN DESK POLICY
91		USER EDUCATION
92	35	GUARDING WORK IN TRANSIT
93	36	<REFER TO FEATURES FOR THREATS 1-13>

[illegible]	[illegible]	<REFER TO FEATURES FOR THREATS [illegible]>
94	37	*GUARDING WORK IN PROGRESS*
95	38	*BUFFER ERASE MECHANISM*
96	39	*PAPER SHREDDER*
97		*USE OF OLD RIBBONS FOR SENSITIVE JOBS*
98		*DESTRUCTION OF CARBON PAPER AND RIBBONS*
99	40	*<REFER TO FEATURES FOR THREATS 41-44>*
100	41	*CAREFUL ADMINISTRATIVE PROCEDURES*
101		*IMPORTANT MAIL SENT REGISTERED OR BY COURIER*
102		*DELIVERY CONFIRMATION*
103	42 43	*SECOND PERSON VERIFICATION*
104		*CHECKSUMS*
105		*SOFTWARE CHECKS*
106	44	*VERIFICATION CHECKS*
107		*CHECKSUMS*
108		*SOFTWARE CHECKS*
109		*ORIGINATOR VERIFICATION*
110	45	*TESTING*
111		*AUDIT PROGRAMS*
112		*TESTING AND VERIFICATION*
113		*PENETRATION ATTEMPTS*
114	46	*PROGRAM TESTING AND VALIDATION*
115	47	*ADEQUATE DOCUMENTATION AND DESIGN SPECS*
116	48 49 50	*ADEQUATE DOCUMENTATION AND DESIGN SPECS*
117		*PROGRAM TESTING AND VALIDATION*
118		*PROGRAMMER EDUCATION*
119	51	*PROGRAM TESTING AND VALIDATION*
120		*CODE INSPECTION, RECOMPILATION*
121		*CHOOSING WRITER WHO COULD NOT BENEFIT*
122	52	*TESTING ON SETUP DATA*
123		*CONTAINMENT OF TEST PROGRAMS*
124	53	*<REFER TO FEATURES FOR THREATS 54-56>*
125	54	*FIRE EXTINGUISHING SYSTEM*
126		*HEAT/SMOKE/FIRE DETECTORS WITH ALARMS*
127		*FIRE EXTINGUISHERS*
128		*AUTOMATIC EXTINGUISHING SYSTEM*
129		*FIRE PROTECTION MEASURES*
130		*FIREWALLS*
131		*FIREPROOF VAULT*
132		*FIRE DRILLS*
133		*FIRE PREVENTION MEASURES*
134		*NO SMOKING POLICY*
135		*USE OF FIRE RESISTANT MATERIALS*
136	55	*FLOOD PREVENTION MEASURES*
137		*ADEQUATE DRAINAGE*
138		*WATER SHUTOFF VALVE*
139		*WATER PROOF MACHINE COVERS*
140		*LOCATION NOT FLOOD-PRONE*
141		*COMPUTER ROOM NOT LOCATED IN THE BASEMENT*
142		*WATER PIPES NOT LOCATED DIRECTLY ABOVE THE EQUIPMENT*

```
143      56            LOCATION NOT ON ACTIVE FAULT
144                    ADEQUATE STRUCTURAL RE-ENFORCEMENT

145      57            COORDINATED PLAN WITH POLICE
146                    <ALSO REFER TO FEATURES FOR THREAT NO. 1>

147      58            SMOKE DETECTORS
148                    <ALSO REFER TO FEATURES FOR THREAT NO. 57>

149      59            FAVORABLE LOCATION CHOICE
150                    <ALSO REFER TO FEATURES FOR THREAT NO. 57>

151      60 61         <REFER TO FEATURES FOR THREAT NO. 57>

152      62            MONITORING EQUIPMENT AND ALARM SYSTEM

153      63            PREVENTIVE MAINTENANCE
154                    HARDWARE CHECKS

155      64            ADEQUATE ADMINISTRATIVE PROCEDURES
156                    BACKUP FACILITIES

157      65            AUXILIARY POWER SUPPLY FOR MACHINE AND SECURITY DEVICES
158                    MACHINE FEATURE FOR GRACEFUL SHUTDOWN ON POWER FAILURE

159      66            POWER SUPPLY LINE FILTER
160                    VOLTAGE STABILIZER FOR POWER SUPPLY
161                    MONITORING SYSTEM WITH ALARM

162      67            ELECTRICAL INSPECTION

163      68            AUXILIARY WATER SUPPLY
164                    FLOW MONITOR WITH ALARM

165      69            WATER FILTERS

166      70            TEMPERATURE CONTROLLERS
167                    TEMPERATURE MONITOR WITH ALARM

168      71            EMERGENCY LIGHTS
169                    AUXILIARY POWER SUPPLY

170      72            ALARM SYSTEM
171                    CONTINGENCY PLANS

172      73            <REFER TO FEATURES FOR THREAT NO. 54>

173      74            WATER TIGHT WINDOWS AND DOORS IN OPERATIONS AREA
174                    <ALSO REFER TO FEATURES FOR THREAT NO. 55>

175      75            <REFER TO FEATURES FOR THREAT NO. 56>

176      76            <REFER TO FEATURES FOR THREAT NO. 57>

177      77            <REFER TO FEATURES FOR THREAT NO. 58>

178      78            <REFER TO FEATURES FOR THREAT NO. 59>

179      79            <REFER TO FEATURES FOR THREAT NO. 60>

180      80            <REFER TO FEATURES FOR THREAT NO. 61>

181      81            PROPER PHYSICAL AREA DESIGN AND CONSTRUCTION

182      82            BACKUP COMMUNICATIONS EQUIPMENT
                       PRACTICED CONTINGENCY PLANS
```

```
183                         PRACTICED CONTINGENCY PLANS

184      83 84              <REFER TO FEATURES FOR THREAT NO. 1>

185      85                 ELECTRICAL SHIELDING
186                              ELECTRICAL SHIELDING OF OPERATIONS AREA
187                              STORAGE OF MAGNETIC MEDIA IN SHIELDING SAFES

188      86                 <REFER TO FEATURES FOR THREAT NO. 1>

189      87                 <REFER TO FEATURES FOR THREAT NO. 1>
190                         SECURE LIBRARY FACILITIES
191                              SECURE TAPE AND DISK LIBRARY
192                              ONLY AUTHORIZED PERSONNEL ALLOWED TO ENTER LIBRARY

193      88                 <REFER TO FEATURES FOR THREAT NO. 1>

194      89                 PAPER SHREDDER
195                         USE OF OLD RIBBONS WITH SENSITIVE JOBS
196                         INCINERATORS
197                         EMPLOYEE AWARENESS AND EDUCATION
198                         SECURE DISPOSAL BINS

199      90                 PAPER SHREDDER
200                         INCINERATORS
201                         EMPLOYEE AWARENESS AND EDUCATION
202                         SECURE DISPOSAL BINS

203      91                 REASONABLE AND INDUSTRY COMPARABLE SALARIES
204                         REFERENCE CHECKING
205                         CAREFUL SUPERVISION

206      92                 REASONABLE AND INDUSTRY COMPARABLE SALARIES
207                         REFERENCE CHECKING
208                         CAREFUL SUPERVISION
209                         EMPLOYEE MORALE PROGRAMS

210      93                 PROMPT EMPLOYEE COMPLAINT HANDLING
211                         <ALSO REFER TO FEATURES FOR THREAT NO. 92>

212      94                 IMMEDIATE NOTICE ON LAYOFF (WITH APPROPRIATE PAY)
213                         PROMPT EMPLOYEE COMPLAINT HANDLING
214                         <REFER ALSO TO FEATURES FOR THREAT NO. 92>

215      95 96 97 98 99     <REFER TO FEATURES FOR THREAT NO. 92>

216      100                ADEQUATE EMPLOYEE TRAINING
217                         <ALSO REFER TO FEATURES FOR THREAT NO. 92>

218      101                REFERENCE CHECKING
219                         LIMIT EMPLOYEE AUTHORITY
220                         NEED TO KNOW POLICY

221      102                REFERENCE CHECKING
222                         CORPORATE INTELLIGENCE

223      103                ADEQUATE EMPLOYEE TRAINING
224                         <ALSO REFER TO FEATURES FOR THREAT NO. 92>

225      104                USE LOG
226                         LIBRARY STORAGE

227      105                USE LOG
228                         LIBRARY STORAGE
229                         CLEAN DESK POLICY

230      106                USE LOG
```

230	106	USE LOG
231		LIBRARY STORAGE
232		CLEAR CLASSIFICATION LABELLING
233		PROPER DISPOSAL
234		CLEAN DESK POLICY
235	107	CLEARLY DEFINED AUTHORIZATION FOR MODIFICATION
236		CLEAR CLASSIFICATION LABELLING
237		CLEAN DESK POLICY
238		USE LOG
239		PROTECTED LIBRARY STORAGE
240	108	GOOD COMMUNICATION SYSTEM BETWEEN THE SITES
241		SIMULATED DISASTER TESTS
242		RECIPROCAL AGREEMENTS BETWEEN COMPANIES (INCLUDES PERSONNEL)
243	109	USE OF SIMILAR EQUIPMENT FOR BACKUP (WITH PERIODIC RECHECKING)
244	110	ADEQUATE EMPLOYEE TRAINING
245		SIMULATED DISASTER TESTS
246	111	(ALSO REFER TO THE SECTION ON HARDWARE)
247	112 113	SIMULATED DISASTER TESTS
248		PROGRAM FOR BACKUP MAINTENANCE
249	114	ADEQUATE EMPLOYEE TRAINING
250		SIMULATED DISASTER TESTS
251	115	DUPLICATE DATA STORED SAFELY
252		SIMULATED DISASTER TESTS
253	116	(SEE ALSO SECTION ON SOFTWARE)
254	117	BACKUP GENERATOR AND FUEL
255	118	BACKUP STORE OF FUEL
256	119	BACKUP STORE OF OPERATIONS MATERIALS
257	120	(SEE ALSO SECTION ON THE COMPUTER CENTER)
258	121	PROPER PLANNING
259		SIMULATED DISASTER TESTS
260	122	CONTINGENCY PLANS FOR REACHING PERSONNEL AWAY FROM WORK
261		SIMULATED DISASTER TESTS
262	123	PROPER PLANNING
263		SIMULATED DISASTER TESTS
264	124	PROGRAM FOR BACKUP MAINTENANCE
265		SIMULATED DISASTER TESTS
266	125	PROPER PLANNING
267		SIMULATED DISASTER TESTS
268	126	PROGRAM FOR BACKUP MAINTENANCE
269		SIMULATED DISASTER TESTS
270		PROPER PLANNING
271	127 128	PROPER PLANNING
272		ADEQUATE EMPLOYEE TRAINING
273		SIMULATED DISASTER TESTS
274	129	(ALSO REFER TO THE SECTION ON DOCUMENTATION)

Appendix B

A Sample Run

We present here an example of the system in use. Included is:

(1) a list of the triples representing the sample installation

(2) input forms--one blank form and a set of completed forms

(3) a terminal session which illustrates the data entry process and use of the analysis functions

Following is a list of the triples representing the sample installation. The threat and feature numbers refer to the names as listed in Appendix A. The format of the triples below is:

object info : object value
threat info : threat likelihood (threat name) threat number
feature info: feature resistance (feature name) feature numbers(s)

1. Hardware

1.1 Central Machine

object info : **very high**
threat info : **medium** (unauthorized use) #8
feature info: **pretty high** (guard) #2

object info : **very high**
threat info : **pretty low** (human error) #10
feature info: **medium** (operator training, documentation) #29 30

1.2 Storage Media

object info : **high**
threat info : **high** (unauthorized read) #13
feature info: **pretty low** (encryption, system protection) #43 44

object info : **high**
threat info : **low** (theft) #11
feature info: **fairly high** (physical access controls) #31

Metering Equipment (add to hierarchy under Hardware)

object info : **low**

threat info : **low** (hardware tampering--modified operation) #4

feature info: **high** (alarmed cabinets) #21

2. Software

object info : **very high**

threat info : **medium** (unauthorized access: read/write) #16

feature info: **medium to pretty high** (authorization and access control mechanism) #46

2.1 Operating System

object info : **high**

threat info : **medium** (defective implementation) #45

feature info: **medium** (testing and verification) #112

2.2 Programs

object info : **medium**

threat info : **fairly high** (inadequate debugging) #46

feature info: **(fairly low) to medium** (testing and validation) #114

2.3 Data

object info : **high**

threat info : **high** (reading of unsecured storage media) #20

feature info: **pretty low** (library facility and use log) #60 61 object info : **high**

threat info : **medium to high** (unauthorized reading of exposed output) #33

feature info: **low** (user and employee diligence) #90 91

object info : **high**

threat info : **pretty high** (data preparation errors) #43

feature info: **high** (verification and edit checks) #103 104 105

2.3.2 Institution Data

object info : **(fairly high) to high**

threat info : **sortof low** (competitor subterfuge) #0

feature info: **low to medium** (legal recourse, employee loyalty, guards) #0

2.3.2.2 Financial Data

object info : **(fairly high) to high**

threat info : **high** (employee theft) #0

feature info: **low** (audit checks) #0

3. The Computer Center

3.1 Resource Supply Systems

object info : **very high**

threat info : **sortof low** (earthquake) #56

feature info: **low** (adequate structural reenforcement) #144

object info : **very high**

threat info : **fairly low** (fire) #54

feature info: **medium** (alarms, extinguishers) #126 127

3.2 The Building

object info : **medium**

threat info : **fairly low** (fire) #73

feature info: **medium** (alarms, extinguishers) #126 127

3.2.2.1 Computer Room

object info : **high**

threat info : **low** (magnets) #84

feature info: **(pretty low) to medium** (guards) #2

object info : **high**

threat info : **medium** (unauthorized intruders) #86

feature info: **pretty high** (guards, alarmed doors) #2 11

OBJECT NO: ____________________

ADD, A name or number ____________________

VALUE, V object value ____________________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

OBJECT NO: ____________________

ADD, A name or number ____________________

VALUE, V object value ____________________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

OBJECT NO: ____________________

ADD, A name or number ____________________

VALUE, V object value ____________________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

OBJECT NO: ____________________

ADD, A name or number ____________________

VALUE, V object value ____________________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

OBJECT NO: 1

ADD, A name or number A METERING EQUIPMENT

VALUE, V object value

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE

OBJECT NO: 11

ADD, A name or number

VALUE, V object value V VERY HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
8	MEDIUM	2	PRETTY HIGH
10	PRETTY LOW	29 30	MEDIUM

OBJECT NO: 12

ADD, A name or number

VALUE, V object value V HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
13	HIGH	43 44	PRETTY LOW
11	LOW	31	FAIRLY HIGH

OBJECT NO: METERING EQUIPMENT

ADD, A name or number

VALUE, V object value V LOW

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
4	LOW	21	HIGH

OBJECT NO: 2

ADD, A name or number ____

VALUE, V object value V VERY HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
16	MEDIUM	46	MEDIUM TO PRETTY HIGH

OBJECT NO: 21

ADD, A name or number ____

VALUE, V object value V HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
45	MEDIUM	112	MEDIUM

OBJECT NO: 22

ADD, A name or number ____

VALUE, V object value V MEDIUM

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
46	FAIRLY HIGH	114	(FAIRLY LOW) TO MEDIUM

OBJECT NO: 23

ADD, A name or number ____

VALUE, V object value V HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
20	HIGH	60 61	PRETTY LOW
33	MEDIUM TO HIGH	90 91	LOW
43	PRETTY HIGH	103 104 105	HIGH

OBJECT NO: 232

ADD, A name or number

VALUE, V object value V (FAIRLY HIGH) TO HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
0	SORTOF LOW	0	LOW TO MEDIUM

OBJECT NO: 2322

ADD, A name or number

VALUE, V object value V (FAIRLY HIGH) TO HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
0	HIGH	0	LOW

OBJECT NO: 31

ADD, A name or number

VALUE, V object value V VERY HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
56	SORTOF LOW	114	LOW
54	FAIRLY LOW	126 127	MEDIUM

OBJECT NO: 32

ADD, A name or number

VALUE, V object value V MEDIUM

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
73	FAIRLY LOW	126 127	MEDIUM

OBJECT NO: 3221

ADD, A name or number ____________

VALUE, V object value V HIGH

THREAT NO	THREAT LIKELIHOOD	FEATURE NOS	FEATURE RESISTANCE
84	LOW	2	(PRETTY LOW) TO MEDIUM
86	MEDIUM	2 11	PRETTY HIGH

OBJECT NO: ____________

ADD, A name or number ____________

VALUE, V object value ____________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

OBJECT NO: ____________

ADD, A name or number ____________

VALUE, V object value ____________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

OBJECT NO: ____________

ADD, A name or number ____________

VALUE, V object value ____________

THREAT NO THREAT LIKELIHOOD FEATURE NOS FEATURE RESISTANCE

```
SECURATE
HI THERE.
PLEASE WAIT A FEW MOMENTS WHILE WE SET THINGS UP.


HI AGAIN.
ENTER THE NAME OF YOUR WORKSPACE ('NONE' FOR THE FIRST TIME):
NONE
DO YOU WANT TO USE A SYSTEM MODEL OTHER THAN THE STANDARD COMPUTER INSTALLATION MODEL? N



YOU ARE NOW ENTERING THE DATA ENTRY PHASE.

DO YOU WANT TO USE THREAT NUMBERS? Y
DO YOU WANT TO USE FEATURE NUMBERS? Y
ENTER A NAME FOR YOUR FILE: EXAMPLE
DO YOU WANT YOUR DATA TO BE ENCRYPTED WHEN IT IS FILED? Y
ENTER A PASSWORD TO BE ASSOCIATED WITH YOUR FILE:
[redacted]
YOU MUST REMEMBER THIS PASSWORD AS YOU WILL NEED TO SPECIFY IT TO ACCESS YOUR DATA AT A LATER DATE.
ENTER THE OBJECT NUMBER FOR THE NEXT OBJECT: 1
HARDWARE
: ADD METERING EQUIPMENT
METERING EQUIPMENT RECEIVED OBJECT NUMBER 71
: O
OBJECT NO 11, CENTRAL MACHINE IS NEXT.
: V VERY HIGH
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
→ 8 MEDIUM 2 PRETTY HIGH
→ 10 PRETTY LOW 29 30 MEDIUM .
→
: N
OBJECT NO 12, STORAGE MEDIA IS NEXT.
: V HIGH
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
→ 13 HIGH 43 44 PRETTY LOW
→ 11 LOW 31 FAIRLY HIGH
→
: N
OBJECT NO 13, COMMUNICATIONS EQUIPMENT IS NEXT.
: N
OBJECT NO 14, I/O DEVICES IS NEXT.
: N
OBJECT NO 71, METERING EQUIPMENT IS NEXT.
: V LOW
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
→ 4 LOW 21 HIGH
→
: N
ENTER THE OBJECT NUMBER FOR THE NEXT OBJECT: 2
SOFTWARE
: V VERY HIGH
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
→ 16 MEDIUM 46 MEDIUM TO PRETTY HIGH
→
: O
OBJECT NO 21, OPERATING SYSTEM IS NEXT.
: V HIGH
```

```
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
+ 45 MEDIUM 112 MEDIUM
+
: N
OBJECT NO 22, PROGRAMS IS NEXT.
: V MEDIUM
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
+ 46 FAIRLY HIGH 114 (FAIRLY LOW) TO MEDIUM
+
: N
OBJECT NO 23, DATA IS NEXT.
: V HIGH
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
+ 20 HIGH 60 61 PRETTY LOW
+ 33 MEDIUM TO HIGH 90 91 LOW
+ 43 PRETTY HIGH 103 104 105 HIGH
+
: O
OBJECT NO 231, PERSONAL DATA IS NEXT.
: N
OBJECT NO 232, INSTITUTION DATA IS NEXT.
: V (FAIRLY HIGH) TO HIGH
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
+ 0 SORTOF LOW 0 LOW TO MEDIUM
+
: O
OBJECT NO 2321, MARKETING DATA IS NEXT.
: N
OBJECT NO 2322, FINANCIAL DATA IS NEXT.
: V (FAIRLY HIGH) TO HIGH
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
+ 0 HGIH 0 LOW
HGIH IS NOT A RECOGNIZABLE WORD.
NO ACTION WAS TAKEN FOR THIS ENTRY.  TRY AGAIN.
+ 0 HIGH 0 LOW
+
: N
OBJECT NO 2323, OPERATIONS DATA IS NEXT.
: N
OBJECT NO 2324, PLANNING DATA IS NEXT.
: N
OBJECT NO 2325, OTHER DATA IS NEXT.
: N
ENTER THE OBJECT NUMBER FOR THE NEXT OBJECT: 3
THE COMPUTER CENTER
: O
OBJECT NO 31, RESOURCE SUPPLY SYSTEMS IS NEXT.
: V VERY HIGH
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
+ 56 SORTOF LOW 114 LOW
+ 54 FAIRLY LOW 126 127 MEDIUM
+
YOUR WORK IS NOW BEING SAVED.
CHECKPOINT: WORK TO THIS POINT HAS BEEN SAVED.
: N
OBJECT NO 32, THE BUILDING IS NEXT.
: V MEDIUM
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
+ 73 FAIRLY LOW 126 127 MEDIUM
+
: O
OBJECT NO 321, THE BUILDING STRUCTURE IS NEXT.
: N
```

```
      DISPLAY.


FOLLOWING IS A LIST OF OBJECTS ADDED, THEIR ASSIGNED OBJECT
NUMBERS, AND THEIR PARENT IN THE HIERARCHY:
OBJECT           OBJECT NO  PARENT
METERING EQUIPMENT  71       1

                        OBJECTS                                THREATS                                 FEATURES

TRIPLE * NUMBER          NAME                  * NUMBER          NAME                  * NUMBER            NAME
  NO   *               VALUE                   *             LIKELIHOOD                *                RESISTANCE
***************************************************************************************************************************
      ***                                     ***                                     ***
1      * 11     CENTRAL MACHINE                * 8      UNAUTHORIZED USE               * 2    GUARD
       *  VERY HIGH                            *   MEDIUM                              *  PRETTY HIGH
      ***                                     ***                                     ***
2      * 11     CENTRAL MACHINE                * 10     HUMAN ERROR                    * 29   OPERATOR TRAINING
       *                                       *                                       * 30   DETAILLED, ACCURATE, ACCESSIBL
       *  VERY HIGH                            *   PRETTY LOW                          *  MEDIUM
      ***                                     ***                                     ***
3      * 12     STORAGE MEDIA                  * 13     UNAUTHORIZED READ              * 43   DATA ENCRYPTION
       *                                       *                                       * 44   EFFECTIVE STORAGE ACCESS CONTR
       *  HIGH                                 *   HIGH                                *  PRETTY LOW
      ***                                     ***                                     ***
4      * 12     STORAGE MEDIA                  * 11     THEFT                          * 31   PHYSICAL ACCESS CONTROLS
       *  HIGH                                 *   LOW                                 *  FAIRLY HIGH
      ***                                     ***                                     ***
5      * 71     METERING EQUIPMENT             * 4      HARDWARE TAMPERING--MODIFIED O* 21   LOCKS AND ALARMS ON MACHINE CO
       *  LOW                                  *   LOW                                 *  HIGH
      ***                                     ***                                     ***
6      * 2      SOFTWARE                       * 16     UNAUTHORIZED ACCESS--R/W/E     * 46   EFFECTIVE AUTHORIZATION AND AC
       *  VERY HIGH                            *   MEDIUM                              *  MEDIUM TO PRETTY HIGH
      ***                                     ***                                     ***
7      * 21     OPERATING SYSTEM               * 45     DEFECTIVE IMPLEMENTATION       * 112  TESTING AND VERIFICATION
       *  HIGH                                 *   MEDIUM                              *  MEDIUM
      ***                                     ***                                     ***
8      * 22     PROGRAMS                       * 46     INADEQUATE DEBUGGING           * 114  PROGRAM TESTING AND VALIDATION
       *  MEDIUM                               *   FAIRLY HIGH                         *  (FAIRLY LOW) TO MEDIUM
      ***                                     ***                                     ***
9      * 23     DATA                           * 20     UNSECURED STORAGE MEDIA        * 60   ADEQUATE AND ENFORCED LIBRARY
       *                                       *                                       * 61   USAGE LOG
       *  HIGH                                 *   HIGH                                *  PRETTY LOW
      ***                                     ***                                     ***
10     * 23     DATA                           * 33     EXPOSED OUTPUT                 * 90   CLEAN DESK POLICY
       *                                       *                                       * 91   USER EDUCATION
       *  HIGH                                 *   MEDIUM TO HIGH                      *  LOW
      ***                                     ***                                     ***
11     * 23     DATA                           * 43     DATA PREPARATION ERRORS        * 103  SECOND PERSON VERIFICATION
       *                                       *                                       * 104  CHECKSUMS
       *                                       *                                       * 105  SOFTWARE CHECKS
       *  HIGH                                 *   PRETTY HIGH                         *  HIGH
      ***                                     ***                                     ***
12     * 232    INSTITUTION DATA               * 0                                     * 0
       *  FAIRLY HIGH TO HIGH                  *   SORTOF LOW                          *  LOW TO MEDIUM
      ***                                     ***                                     ***
13     * 2322   FINANCIAL DATA                 * 0                                     * 0
       *  FAIRLY HIGH TO HIGH                  *   HIGH                                *  LOW
      ***                                     ***                                     ***
14     * 31     RESOURCE SUPPLY SYSTEMS        * 56     EARTHQUAKE                     * 144  ADEQUATE STRUCTURAL RE-ENFORCE
       *  VERY HIGH                            *   SORTOF LOW                          *  LOW
      ***                                     ***                                     ***
```

```
OBJECT NO 322, COMPUTER OPERATIONS AREA IS NEXT.
: O
OBJECT NO 3221, COMPUTER ROOM IS NEXT.
: V HIGH
THREAT NO  THREAT LIKELIHOOD  FEATURE NOS  FEATURE RESISTANCE
→ 84 LOW 2 (PRETTY LOW) TO MEDIUM
→ 86 MEDIUM 2 11 PRETTY HIGH
→
: N
OBJECT NO 3222, DATA RECEPTION AREA IS NEXT.
: N
OBJECT NO 3223, TAPE AND DISK LIBRARY IS NEXT.
: N
OBJECT NO 3224, CE ROOM IS NEXT.
: N
OBJECT NO 3225, DATA PREPARATION AREA IS NEXT.
: N
OBJECT NO 3226, PHYSICAL PLANT ROOM IS NEXT.
: N
OBJECT NO 3227, STATIONERY STORAGE IS NEXT.
: N
OBJECT NO 33, WASTE MATERIALS IS NEXT.
: N
ENTER THE OBJECT NUMBER FOR THE NEXT OBJECT: 0
DO YOU WANT TO ADD ANY MORE OBJECTS WHICH ARE NOT IN THE HIERARCHY? N
YOUR WORK IS NOW BEING SAVED.
CHECKPOINT: WORK TO THIS POINT HAS BEEN SAVED.
TO RECEIVE INSTRUCTIONS IN USING THE ANALYSIS FUNCTIONS, ENTER 'INSTRUCTIONS'.
```

```
     INSTRUCTIONS
    THE FOLLOWING ANALYSIS FUNCTIONS ARE AVAILABLE. TO INVOKE SIMPLY TYPE IN THE NAME

    OVERALLRATING -- THIS FUNCTION WILL RATE THE ENTIRE INSTALLATION. THE RATING WILL THEN
      (ALSO ORATE)     BE PRINTED OUT

    SECTIONRATINGS -- THIS FUNCTION WILL RATE THE SUBSECTIONS OF A SPECIFIED OBJECT SECTION.
      (ALSO SRATE)      FOR EXAMPLE IF HARDWARE, OBJECT 1, IS SPECIFIED, THIS FUNCTION WILL RETURN
                        RATINGS FOR EACH OF THE MAIN SUBSECTIONS OF HARDWARE: THE CENTRAL MACHINE,
                        STORAGE MEDIA, COMMUNICATIONS EQUIPMENT, AND I/O DEVICES.

    INDIVIDUALRATING -- THIS FUNCTION WILL RETURN THE RATING FOR A SPECIFIED SUBSECTION OF THE HIERARCHY.
      (ALSO IRATE)
    WORSTSUBSECTION -- THIS FUNCTION WILL EVALUATE THE SUBSECTIONS OF EITHER THE ENTIRE INSTALLATION OR
      (ALSO WRATE)       A SPECIFIED SUBSECTION OF THE INSTALLATION AND PRINT OUT THAT SUBSECTION WITH
                         THE LOWEST RATING.
DO YOU WANT TO SEE A DESCRIPTION OF THE RATING FUNCTIONS? Y

   THE FOLLOWING RATING FUNCTIONS ARE AVAILABLE:
     1) WEAKEST LINK
     2) SELECTED WEAKEST LINK
     3) FUZZY MEAN
     4) FUZZY MEAN WEIGHTED BY VALUE
     5) FUZZY MEAN WITH EACH MAJOR SUBSECTION WEIGHTED BY MAXIMUM OBJECT VALUE

ENTER THE NUMBER OF THE RATING FUNCTION YOU WISH TO USE: 3
```

```
15       * 31      RESOURCE SUPPLY SYSTEMS          * 54      FIRE                             * 126  HEAT/SMOKE/FIRE DETECTORS WITH
         *                                          *                                          * 127  FIRE EXTINGUISHERS
         *  VERY HIGH                               *   FAIRLY LOW                             *  MEDIUM
        ***                                        ***                                        ***
16       * 32      THE BUILDING                     * 73      FIRE                             * 126  HEAT/SMOKE/FIRE DETECTORS WITH
         *                                          *                                          * 127  FIRE EXTINGUISHERS
         *  MEDIUM                                  *   FAIRLY LOW                             *  MEDIUM
        ***                                        ***                                        ***
17       * 3221    COMPUTER ROOM                    * 84      MAGNETS                          * 2    GUARD
         *  HIGH                                    *   LOW                                    *  (PRETTY LOW) TO MEDIUM
        ***                                        ***                                        ***
18       * 3221    COMPUTER ROOM                    * 86      UNAUTHORIZED INTRUDERS           * 2    GUARD
         *                                          *                                          * 11   ALARM SYSTEM
         *  HIGH                                    *   MEDIUM                                 *  PRETTY HIGH
```

```
      RATESET
DO YOU WANT TO SEE A DESCRIPTION OF THE RATING FUNCTIONS? Y

   THE FOLLOWING RATING FUNCTIONS ARE AVAILABLE:
     1) WEAKEST LINK
     2) SELECTED WEAKEST LINK
     3) FUZZY MEAN
     4) FUZZY MEAN WEIGHTED BY VALUE
     5) FUZZY MEAN WITH EACH MAJOR SUBSECTION WEIGHTED BY MAXIMUM OBJECT VALUE

ENTER THE NUMBER OF THE RATING FUNCTION YOU WISH TO USE: 1
      OVERALLRATING


**********************************************************************
*
*  NAME                    RATING (USING WEAKEST LINK)
*
*  THE INSTALLATION          LOW
*
**********************************************************************



      RATESET
DO YOU WANT TO SEE A DESCRIPTION OF THE RATING FUNCTIONS? N
ENTER THE NUMBER OF THE RATING FUNCTION YOU WISH TO USE: 2
      SECTIONALRATING
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 0
SPECIFY MINIMUM FOR HARDWARE : MEDIUM
4 ELEMENT(S) USED
SPECIFY MINIMUM FOR SOFTWARE : HIGH
1 ELEMENT(S) USED
SPECIFY MINIMUM FOR THE COMPUTER CENTER : PRETTY HIGH
4 ELEMENT(S) USED


**********************************************************************
*
*  NAME                    RATING (USING SELECTED WEAKEST LINK)
*
*  HARDWARE                   PRETTY LOW
*  SOFTWARE                   PRETTY HIGH
*  THE COMPUTER CENTER        PRETTY HIGH
*
**********************************************************************


      SETRATE 1
      SRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 0


**********************************************************************
*
*  NAME                    RATING (USING WEAKEST LINK)
*
*  HARDWARE                   PRETTY LOW
*  SOFTWARE                   LOW
*  THE COMPUTER CENTER        LOW
*
```

```
*
*************************************************************************


      SETRATE 3
      ORATE


*************************************************************************
*
*  NAME                     RATING (USING FUZZY MEAN)
*
*  THE INSTALLATION            EXTREMELY MEDIUM
*
*************************************************************************


      WORSTSUBSECTION
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 0


*************************************************************************
*
*  NAME                     RATING (USING FUZZY MEAN)
*
*  HARDWARE                    ((SLIGHTLY LOWER ) THAN FAIRLY HIGH )AND (SLIGHTLY HIGHER ) THAN SORTOF HIGH
*  SOFTWARE                    SORTOF MEDIUM
*  THE COMPUTER CENTER         VERY MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       SOFTWARE
*
*************************************************************************


      WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 2


*************************************************************************
*
*  NAME                     RATING (USING FUZZY MEAN)
*
*  OPERATING SYSTEM            MOREORLESS MEDIUM
*  PROGRAMS                    MOREORLESS MEDIUM
*  DATA                        SORTOF MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       DATA
*
*************************************************************************


      SETRATE 4
      WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 2
```

```
************************************************************************
*
*  NAME                  RATING (USING FUZZY MEAN WEIGHTED BY VALUE)
*
*  OPERATING SYSTEM         (MOREORLESS MEDIUM ) TO (SORTOF HIGH )
*  PROGRAMS                 MOREORLESS MEDIUM
*  DATA                     SORTOF MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       DATA
*
************************************************************************
```

```
      MODTRIP
ENTER THE TRIPLE NUMBER: 10
ENTER THE NUMBER OF THE CATEGORY TO BE MODIFIED-
     1) OBJECT NUMBER
     2) THREAT NUMBER
     3) FEATURE NUMBER(S)
     4) OBJECT VALUE
     5) THREAT LIKLIHOOD
     6) FEATURE RESISTANCE
: 6
ENTER THE NEW FEATURE RESISTANCE: MEDIUM

      DISPLAY


FOLLOWING IS A LIST OF OBJECTS ADDED, THEIR ASSIGNED OBJECT
NUMBERS, AND THEIR PARENT IN THE HIERARCHY:
OBJECT            OBJECT NO  PARENT
METERING EQUIPMENT  71       1

                        OBJECTS                               THREATS                               FEATURES

TRIPLE * NUMBER           NAME                * NUMBER          NAME                  * NUMBER           NAME
 NO    *               VALUE                  *           . LIKELIHOOD                *             RESISTANCE
**************************************************************************************************************************
      ***                                    ***                                     ***
1      * 11     CENTRAL MACHINE               * 8      UNAUTHORIZED USE               * 2    GUARD
       *  VERY HIGH                           *   MEDIUM                              *  PRETTY HIGH
      ***                                    ***                                     ***
2      * 11     CENTRAL MACHINE               * 10     HUMAN ERROR                    * 29   OPERATOR TRAINING
       *                                      *                                       * 30   DETAILLED, ACCURATE, ACCESSIBL
       *  VERY HIGH                           *   PRETTY LOW                          *  MEDIUM
      ***                                    ***                                     ***
3      * 12     STORAGE MEDIA                 * 13     UNAUTHORIZED READ              * 43   DATA ENCRYPTION
       *                                      *                                       * 44   EFFECTIVE STORAGE ACCESS CONTR
       *  HIGH                                *   HIGH                                *  PRETTY LOW
      ***                                    ***                                     ***
4      * 12     STORAGE MEDIA                 * 11     THEFT                          * 31   PHYSICAL ACCESS CONTROLS
       *  HIGH                                *   LOW                                 *  FAIRLY HIGH
      ***                                    ***                                     ***
5      * 71     METERING EQUIPMENT            * 4      HARDWARE TAMPERING--MODIFIED O* 21   LOCKS AND ALARMS ON MACHINE CO
       *  LOW                                 *   LOW                                 *  HIGH
      ***                                    ***                                     ***
6      * 2      SOFTWARE                      * 16     UNAUTHORIZED ACCESS--R/W/E     * 46   EFFECTIVE AUTHORIZATION AND AC
       *  VERY HIGH                           *   MEDIUM                              *  MEDIUM TO PRETTY HIGH
      ***                                    ***                                     ***
7      * 21     OPERATING SYSTEM              * 45     DEFECTIVE IMPLEMENTATION       * 112  TESTING AND VERIFICATION
       *  HIGH                                *   MEDIUM                              *  MEDIUM
      ***                                    ***                                     ***
8      * 22     PROGRAMS                      * 46     INADEQUATE DEBUGGING           * 114  PROGRAM TESTING AND VALIDATION
       *  MEDIUM                              *   FAIRLY HIGH                         *  (FAIRLY LOW) TO MEDIUM
      ***                                    ***                                     ***
9      * 23     DATA                          * 20     UNSECURED STORAGE MEDIA        * 60   ADEQUATE AND ENFORCED LIBRARY
       *                                      *                                       * 61   USAGE LOG
       *  HIGH                                *   HIGH                                *  PRETTY LOW
      ***                                    ***                                     ***
10     * 23     DATA                          * 33     EXPOSED OUTPUT                 * 90   CLEAN DESK POLICY
       *                                      *                                       * 91   USER EDUCATION
       *  HIGH                                *   MEDIUM TO HIGH                      *  MEDIUM
      ***                                    ***                                     ***
```

```
11     * 23     DATA                      * 43     DATA PREPARATION ERRORS      * 103  SECOND PERSON VERIFICATION
       *                                  *                                     * 104  CHECKSUMS
       *                                  *                                     * 105  SOFTWARE CHECKS
       *  HIGH                            *   PRETTY HIGH                       *  HIGH
      ***                                ***                                   ***
12     * 232    INSTITUTION DATA          * 0                                   * 0
       *  FAIRLY HIGH TO HIGH             *   SORTOF LOW                        *  LOW TO MEDIUM
      ***                                ***                                   ***
13     * 2322   FINANCIAL DATA            * 0                                   * 0
       *  FAIRLY HIGH TO HIGH             *   HIGH                              *  LOW
      ***                                ***                                   ***
14     * 31     RESOURCE SUPPLY SYSTEMS   * 56     EARTHQUAKE                   * 144  ADEQUATE STRUCTURAL RE-ENFORCE
       *  VERY HIGH                       *   SORTOF LOW                        *  LOW
      ***                                ***                                   ***
15     * 31     RESOURCE SUPPLY SYSTEMS   * 54     FIRE                         * 126  HEAT/SMOKE/FIRE DETECTORS WITH
       *                                  *                                     * 127  FIRE EXTINGUISHERS
       *  VERY HIGH                       *   FAIRLY LOW                        *  MEDIUM
      ***                                ***                                   ***
16     * 32     THE BUILDING              * 73     FIRE                         * 126  HEAT/SMOKE/FIRE DETECTORS WITH
       *                                  *                                     * 127  FIRE EXTINGUISHERS
       *  MEDIUM                          *   FAIRLY LOW                        *  MEDIUM
      ***                                ***                                   ***
17     * 3221   COMPUTER ROOM             * 84     MAGNETS                      * 2    GUARD
       *  HIGH                            *   LOW                               *  (PRETTY LOW) TO MEDIUM
      ***                                ***                                   ***
18     * 3221   COMPUTER ROOM             * 86     UNAUTHORIZED INTRUDERS       * 2    GUARD
       *                                  *                                     * 11   ALARM SYSTEM
       *  HIGH                            *   MEDIUM                            *  PRETTY HIGH


      SETRATE 3

      WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 2


***********************************************************************
*
*  NAME                    RATING (USING FUZZY MEAN)
*
*  OPERATING SYSTEM           MOREORLESS MEDIUM
*  PROGRAMS                   MOREORLESS MEDIUM
*  DATA                       SORTOF MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       DATA
*
***********************************************************************


      MODTRIP
ENTER THE TRIPLE NUMBER: 9
ENTER THE NUMBER OF THE CATEGORY TO BE MODIFIED-
     1) OBJECT NUMBER
     2) THREAT NUMBER
     3) FEATURE NUMBER(S)
     4) OBJECT VALUE
     5) THREAT LIKLIHOOD
     6) FEATURE RESISTANCE
: 6
ENTER THE NEW FEATURE RESISTANCE: MEDIUM
```

```
      WRATE
ENTER THE PARENT OBJECT NUMBER (0 FOR THE TOP LEVEL IN THE HIERARCHY): 2


************************************************************************
*
*  NAME                     RATING (USING FUZZY MEAN)
*
*  OPERATING SYSTEM            MOREORLESS MEDIUM
*  PROGRAMS                    MOREORLESS MEDIUM
*  DATA                        MEDIUM
*
*  THE LOWEST RATING WAS GIVEN TO:
*       OPERATING SYSTEM
*       PROGRAMS
*
************************************************************************
```

Appendix C

Formal Language Definition

```
<sentence> ::= <compound phrase> | <simple phrase>

<compound phrase> ::= <conjunctive phrase> | <range phrase>

<simple phrase> ::= <relational phrase> | <hedged primary>

<conjunctive phrase> ::= <relational phrase> AND <relational phrase>

<range phrase> ::= <hedged primary> TO <hedged primary>

<relational phrase> ::= <composite relation> THAN <hedged primary>

<composite relation> ::= <relation hedge> <relation> | <relation>

<relation hedge> ::= NOT | MUCH | SLIGHTLY

<relation> ::= LOWER | HIGHER

<hedged primary> ::= <hedge> <primary> | <primary> | <fuzzy number>

<hedge> ::= NOT | VERY | MOREORLESS | QUITE | PRETTY |

                   SORTOF | REALLY | EXTREMELY | INDEED

<primary> ::= LOW | HIGH | MEDIUM

<fuzzy number> ::= <fuzzifier> <number>

<fuzzifier> ::= ABOUT

<number> ::= 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |.9 | 10
```

Some of the rating phrases which may be generated with this grammar are:

```
        high
        low
        medium
        not high
        moreorless medium
        indeed low
        low to medium
       (about 4) to about 6
        slightly lower than pretty high
        not higher than medium
       (much higher than low) and slightly lower than sortof high
```

Appendix D

Available Installation Models

There are at present two installation models:

1) The standard computer installation model.

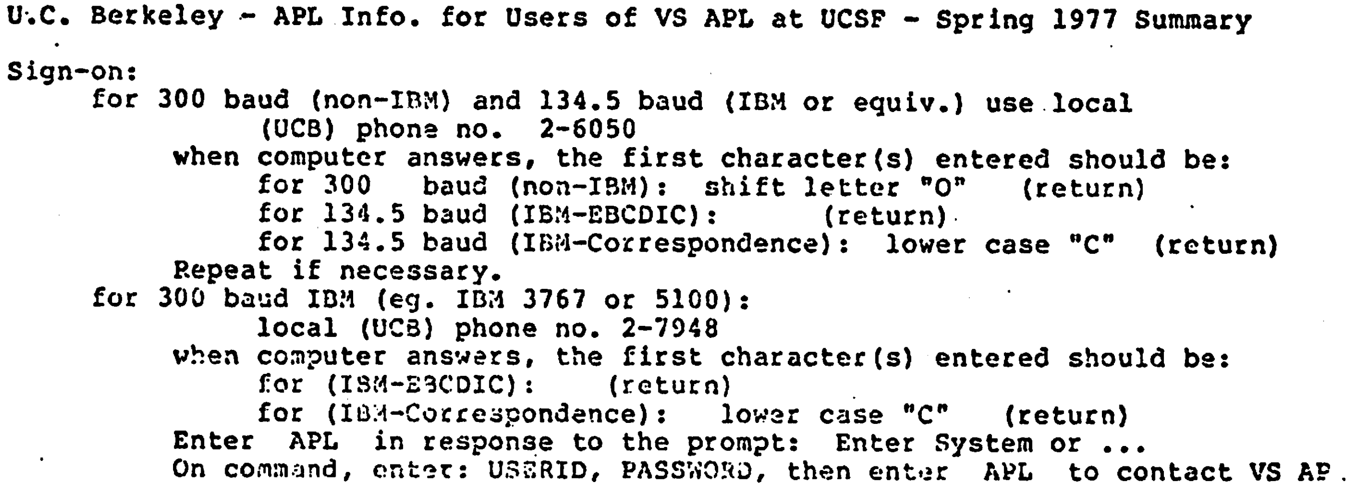
2) A nuclear reactor model. As of July 1977, this is just a small prototype model.

Appendix E

Additional Notes

Logging On

Refer to the figure below for instructions for logging onto the UCSF 370/145. You may safely ignore the various system messages which will be printed out before you enter SECURATE.



```
U.C. Berkeley - APL Info. for Users of VS APL at UCSF - Spring 1977 Summary

Sign-on:
    for 300 baud (non-IBM) and 134.5 baud (IBM or equiv.) use local
            (UCB) phone no.  2-6050
        when computer answers, the first character(s) entered should be:
            for 300   baud (non-IBM):  shift letter "O"   (return)
            for 134.5 baud (IBM-EBCDIC):        (return)
            for 134.5 baud (IBM-Correspondence):  lower case "C"  (return)
        Repeat if necessary.
    for 300 baud IBM (eg. IBM 3767 or 5100):
            local (UCB) phone no. 2-7948
        when computer answers, the first character(s) entered should be:
            for (IBM-EBCDIC):    (return)
            for (IBM-Correspondence):   lower case "C"   (return)
        Enter  APL  in response to the prompt:  Enter System or ...
        On command, enter: USERID, PASSWORD, then enter  APL  to contact VS AP.
```

Logging off

To log off the system when in the APL environment (where you will be when using SECURATE), enter ")OFF". To log off when in the CMS environment (where you'll be right after you log on, but before you call SECURATE), enter "log".

Error Correction

To correct an error in a line you have typed (before you've hit the return key), do the following:

1) Backspace to the leftmost incorrect character.

2) Press the attention button. This may be marked "ATTN" or "BREAK".

3) After the computer does a vertical space, prints a carrot, and does another vertical space, continue with the line from that point.

Note that the above steps will only work in the APL environment. In CMS, a "@" will delete everything in the line to that point, and a backspace will delete the previous character.

Alternative Function Calls

An alternative way to call SRATE, IRATE, and WRATE is to prepend an "S" to the function name and continue with the relevent object number on the same line. This relieves the necessity of responding to a prompt for the object number.

Examples of legal calls are:

```
SSRATE 1
SIRATE 21
SWRATE 33
```

If you would like a message printed out when executing the SAVE function, enter "MESSAVE", instead. This will print out "CHECKPOINT: WORK TO THIS POINT HAS BEEN SAVED." when the save is complete.

CP

Occasionally, when the computer system is having a bad day, you will notice that suddenly all you get are "?CP" messages, no matter what you type in. This means that you were thrown into the virtual machine monitor (CP). The most common cause for this is that you tried to type before the system was ready for it (although this only happens on some terminals and only when the system is heavily loaded). The remedy for this is to enter "BEGIN"; this will put you back in APL. After waiting a couple of moments, you may continue normally, where you left off. Note however, that you will need to retype the input line which caused the problem. If after entering "BEGIN" the system responds by printing an error message, followed by a line number and an APL statement, enter a right pointing arrow "→" followed by the line number that was printed out. At this point you should be able to continue normally.

SECURATE QUICK REFERENCE GUIDE

THE LANGUAGE

Primary Terms

high
low
medium

Primary Hedges

extremely
very
pretty
fairly
sortof

Relations

lower than
higher than

Relation Hedges

not
much
slightly

Connectives

and
to

Additionally, a number from one to ten may be specified, optionally preceded by "**about**". If a number is used, it must be spelled out in letters.

DATA ENTRY

The following commands may be entered following a ":" prompt:

ADD <object name>
VALUE <object value>
NEXT
OFFSPRING
OUT

With the exception of **OUT**, the above commands may be shortened to the first letter.

SECURITY EVALUATION FUNCTIONS

The following commands may be entered:

OVERALLRATING (or **ORATE**)
INDIVIDUALRATING (or **IRATE**)
SECTIONALRATING (or **SRATE**)
WORSTSUBSECTION (or **WRATE**)

Scoring Options

The following scoring options are available and may be specified by entering either "**SETRATE**", followed by a prompt, or just "**RATESET**":

1) Weakest Link
2) Selected Weakest Link
3) Fuzzy Mean
4) Weighted Fuzzy Mean
5) Fuzzy Mean With Each Major Subsection Weighted By Maximum Object Value

Other Functions

ADDTRIP
DELTRIP
MODTRIP
SAVE
HIERARCHY
THREATS
FEATURES