SECURATE QUICK REFERENCE GUIDE

THE LANGUAGE

<table>
<thead>
<tr>
<th>Primary Terms</th>
<th>Primary Hedges</th>
<th>Relations</th>
</tr>
</thead>
<tbody>
<tr>
<td>high</td>
<td>extremely</td>
<td>lower than</td>
</tr>
<tr>
<td>low</td>
<td>very</td>
<td>higher than</td>
</tr>
<tr>
<td>medium</td>
<td>pretty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>fairly</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sortof</td>
<td></td>
</tr>
</tbody>
</table>

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

1. Introduction
2. The Language
3. Initialization and Data Entry
4. Use of Analysis Functions

Appendix A. Object Hierarchy and Threats, Features, and Flaws Listings
Appendix B. A Complete Example
Appendix C. Formal Language Definition
Appendix D. Available Installation Models
Appendix E. Additional Notes

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:

<table>
<thead>
<tr>
<th>Primary Terms</th>
<th>Primary Hedges</th>
<th>Relations</th>
</tr>
</thead>
<tbody>
<tr>
<td>high</td>
<td>extremely</td>
<td>lower than</td>
</tr>
<tr>
<td>low</td>
<td>very</td>
<td>higher than</td>
</tr>
<tr>
<td>medium</td>
<td>pretty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>fairly</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sortof</td>
<td></td>
</tr>
</tbody>
</table>

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
- more or less 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 sort of 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 "sort of", "fairly", and "pretty" shift the curve toward the middle, "sort of" 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):
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:

YOU 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: secure

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:
  0

Object no 11, central machine is next:
  v very high

Threat no threat likelihood feature nos feature resistance
  + 6 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:
  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
Figure 3.2a continued
### Table: Objects, Threats, and Features

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Value</th>
<th>Number</th>
<th>Name</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Central Machine</td>
<td>Very High</td>
<td>3</td>
<td>Unauthorized Use</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Central Machine</td>
<td>Very High</td>
<td>10</td>
<td>Human Error</td>
<td>PRETTY LOW</td>
</tr>
<tr>
<td>3</td>
<td>Storage Media</td>
<td>High</td>
<td>12</td>
<td>Unauthorized Read</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Storage Media</td>
<td>High</td>
<td>11</td>
<td>Theft</td>
<td>LOW</td>
</tr>
<tr>
<td>5</td>
<td>Metering Equipment</td>
<td>Low</td>
<td>22</td>
<td>Programs</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>6</td>
<td>Programs</td>
<td>MEDIUM</td>
<td>32</td>
<td>Hardware Tampering--Modified</td>
<td>LOW</td>
</tr>
<tr>
<td>7</td>
<td>Data</td>
<td>HIGH</td>
<td>20</td>
<td>Inadequate Debugging</td>
<td>FAIRLY HIGH</td>
</tr>
<tr>
<td>8</td>
<td>Data</td>
<td>HIGH</td>
<td>33</td>
<td>Exposed Output</td>
<td>MEDIUM TO HIGH</td>
</tr>
<tr>
<td>9</td>
<td>Data</td>
<td>HIGH</td>
<td>33</td>
<td>Data Preparation Errors</td>
<td>PRETTY HIGH</td>
</tr>
</tbody>
</table>

**Features:**

- Guard: PRETTY HIGH
- Operator Training: PRETTY LOW
- Detailed, Accurate, Accessible: MEDIUM
- Data Encryption: PRETTY LOW
- Effective Storage Access Controls: FAIRLY HIGH
- Physical Access Controls: FAIRLY HIGH
- Locks and Alarms on Machine: HIGH
- Program Testing and Validation: FAIRLY LOW TO MEDIUM
- Adequate and Enforced Library: PRETTY LOW
- Usage Log: PRETTY LOW
- Clean Desk Policy: LOW
- User Education: PRETTY LOW
- Second Person Verification: PRETTY LOW
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.

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

**OFFSPRING**--the system will continue by prompting the user with the previous object's offspring, or, if none, its siblings. 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 periodically 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 |

| 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:

<table>
<thead>
<tr>
<th>VALUE, V object value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A METERING EQUIPMENT</td>
</tr>
</tbody>
</table>

## THREAT NO | THREAT LIKELIHOOD | FEATURE NOS | FEATURE RESISTANCE |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## OBJECT NO:

<table>
<thead>
<tr>
<th>VALUE, V object value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A name or number</td>
</tr>
</tbody>
</table>

## THREAT NO | THREAT LIKELIHOOD | FEATURE NOS | FEATURE RESISTANCE |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>MEDIUM</td>
<td>2</td>
<td>PRETTY HIGH</td>
</tr>
<tr>
<td>10</td>
<td>PRETTY LOW</td>
<td>29 30</td>
<td>MEDIUM</td>
</tr>
</tbody>
</table>

## OBJECT NO:

<table>
<thead>
<tr>
<th>VALUE, V object value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A name or number</td>
</tr>
</tbody>
</table>

## THREAT NO | THREAT LIKELIHOOD | FEATURE NOS | FEATURE RESISTANCE |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>HIGH</td>
<td>43 44</td>
<td>PRETTY LOW</td>
</tr>
<tr>
<td>11</td>
<td>LOW</td>
<td>31</td>
<td>FAIRLY HIGH</td>
</tr>
</tbody>
</table>

## OBJECT NO:

<table>
<thead>
<tr>
<th>VALUE, V object value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A name or number</td>
</tr>
</tbody>
</table>

## THREAT NO | THREAT LIKELIHOOD | FEATURE NOS | FEATURE RESISTANCE |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>LOW</td>
<td>21</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

---

Figure 3.3b Input form completed before logging on
<table>
<thead>
<tr>
<th>OBJECT NO:</th>
<th>ADD, A name or number</th>
<th>VALUE, V object value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>THREAT NO</th>
<th>THREAT LIKELIHOOD</th>
<th>FEATURE NOS</th>
<th>FEATURE RESISTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>FAIRLY HIGH</td>
<td>114</td>
<td>(FAIRLY LOW) TO MEDIUM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBJECT NO:</th>
<th>ADD, A name or number</th>
<th>VALUE, V object value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>THREAT NO</th>
<th>THREAT LIKELIHOOD</th>
<th>FEATURE NOS</th>
<th>FEATURE RESISTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>HIGH</td>
<td>60 61</td>
<td>PRETTY LOW</td>
</tr>
<tr>
<td>33</td>
<td>MEDIUM TO HIGH</td>
<td>90 91</td>
<td>LOW</td>
</tr>
<tr>
<td>43</td>
<td>PRETTY HIGH</td>
<td>103 104 105</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBJECT NO:</th>
<th>ADD, A name or number</th>
<th>VALUE, V object value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>THREAT NO</th>
<th>THREAT LIKELIHOOD</th>
<th>FEATURE NOS</th>
<th>FEATURE RESISTANCE</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>OBJECT NO:</th>
<th>ADD, A name or number</th>
<th>VALUE, V object value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>THREAT NO</th>
<th>THREAT LIKELIHOOD</th>
<th>FEATURE NOS</th>
<th>FEATURE RESISTANCE</th>
</tr>
</thead>
</table>


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.
### Objects

<table>
<thead>
<tr>
<th>Object</th>
<th>Number</th>
<th>Name</th>
<th>Value</th>
<th>Threats</th>
<th>Number</th>
<th>Name</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Machine</td>
<td>1</td>
<td>Very High</td>
<td></td>
<td></td>
<td>1</td>
<td>Unauthorized Use</td>
<td>Medium</td>
</tr>
<tr>
<td>Central Machine</td>
<td>1</td>
<td>Very High</td>
<td></td>
<td></td>
<td>1</td>
<td>Human Error</td>
<td>Pretty Low</td>
</tr>
<tr>
<td>Central Machine</td>
<td>1</td>
<td>High</td>
<td></td>
<td></td>
<td>1</td>
<td>Unauthorized Read</td>
<td>High</td>
</tr>
<tr>
<td>Storage Media</td>
<td>12</td>
<td>High</td>
<td></td>
<td></td>
<td>12</td>
<td>Theft</td>
<td>Low</td>
</tr>
<tr>
<td>Storage Media</td>
<td>12</td>
<td>High</td>
<td></td>
<td></td>
<td>12</td>
<td>Theft</td>
<td>Low</td>
</tr>
<tr>
<td>Metering Equipment</td>
<td>71</td>
<td>Low</td>
<td></td>
<td></td>
<td>71</td>
<td>Hardware Tampering</td>
<td>Medium</td>
</tr>
<tr>
<td>Programs</td>
<td>22</td>
<td>Medium</td>
<td></td>
<td></td>
<td>22</td>
<td>Inadequate Debugging</td>
<td>Fairly High</td>
</tr>
<tr>
<td>Data</td>
<td>23</td>
<td>High</td>
<td></td>
<td></td>
<td>23</td>
<td>Unsecured Storage Media</td>
<td>High</td>
</tr>
<tr>
<td>Data</td>
<td>23</td>
<td>High</td>
<td></td>
<td></td>
<td>23</td>
<td>Exposed Output</td>
<td>Medium to High</td>
</tr>
<tr>
<td>Data</td>
<td>23</td>
<td>High</td>
<td></td>
<td></td>
<td>23</td>
<td>Data Preparation Errors</td>
<td>Pretty High</td>
</tr>
</tbody>
</table>

### Features

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Guard</td>
<td>Pretty High</td>
</tr>
<tr>
<td>29</td>
<td>Operator Training</td>
<td>Medium</td>
</tr>
<tr>
<td>30</td>
<td>Detailed, Accurate, Accessible</td>
<td>Medium</td>
</tr>
<tr>
<td>42</td>
<td>Data Encryption</td>
<td>Pretty Low</td>
</tr>
<tr>
<td>43</td>
<td>Effective Storage Access Controls</td>
<td>Pretty Low</td>
</tr>
<tr>
<td>51</td>
<td>Physical Access Controls</td>
<td>Fairly High</td>
</tr>
<tr>
<td>31</td>
<td>Locks and Alarms on Machine CO</td>
<td>High</td>
</tr>
<tr>
<td>114</td>
<td>Program Testing and Validation</td>
<td>(Fairly Low) to Medium</td>
</tr>
<tr>
<td>50</td>
<td>Adequate and Enforced Library</td>
<td>Pretty Low</td>
</tr>
<tr>
<td>90</td>
<td>Clean Desk Policy</td>
<td>Low</td>
</tr>
<tr>
<td>91</td>
<td>User Education</td>
<td>Low</td>
</tr>
<tr>
<td>103</td>
<td>Second Person Verification</td>
<td>High</td>
</tr>
<tr>
<td>104</td>
<td>Checksuns</td>
<td>High</td>
</tr>
<tr>
<td>105</td>
<td>Software Checks</td>
<td>High</td>
</tr>
</tbody>
</table>
RATESST
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) FUZZI MEAN
4) FUZZI MEAN WEIGHTED BY VALUE
5) FUZZI MEAN WITH EACH MAJOR SUBSECTION WEIGHTED BY MAXIMUM OBJECT VALUE

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

OVERALL RATING

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

WORST SUBSECTION
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 *
******************************************************************************

SET RATING 3
INDIVIDUAL RATING
ENTER THE NUMBER OF THE OBJECT TO BE RATED: 2

******************************************************************************
* NAME               RATING (USING FUZZI MEAN)                          *
* SOFTWARE           MEDIUM                                           *
******************************************************************************

Figure 4.1b Use of the security evaluation functions
**SECTIONAL RATING**

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

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

**SECTION 2**

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

SPECIFY MINIMUM FOR HARDWARE : PRETTI HIGH
4 ELEMENT(S) USED
SPECIFY MINIMUM FOR SOFTWARE : PRETTI HIGH
3 ELEMENT(S) USED

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

**SECTION 3**

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

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

Figure 4.1c Continued use of the security evaluation functions
Figure 4.1d Use of the MODTRIP function and the security evaluation functions
DISPLAt
POLLOUIMG IS A LIST OP OBJBCTS ADDSD^ TBSIR
SUHBSRS, ABO TBSIR PARSBf IB TBS BIBRBAt
auBQz * aussz la
NETSRIBG SQUIPMSSf 71 1
Z&LPl * BUBBBR
sa
aaaatai
BAMS
LIK8LIB0O
8 OBAUTBORIZSD 088
II8DIUB
* 10 aOBAB 8R80R
PR8TTI LOB
i
13 OBAOTBORItSD 88AD
BIGB
t
11 TB8PT
LOB
H BARDBAR8 TAMPSRIBG--MODIPIBD
LOB
H BARAD800ATB D8B0GGIBG
PAIRLX BIGB'
20 OB8C0RD 8T0RAGB MBDIA
BIGB
r
93 8XP088D OO^POT
M8DI0M TO BIGB
r
33 DATA PR8PARATI0B BRR0B8
PRBTTI LOB
**•
« 31 PBISICAL ACC888 C0BTR0L8
PAIRLI BIGB
**•
0* 21 LOCKS ABD ALARMS ON MACHINE CO
HIGH
**•
*** 103 SECOND PERSON VERIFICATION
104 CHECKSUNS
105 SOFTWARE CHECKS
HIGH

Figure 4.1e Another data display
WHAT

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

******************************************************************************
• NAME  RATING (USING Fuzzy Mean)
• PROGRAMS  (SORTOP MEDIUM ) TO (MORSELESS MEDIUM )
• DATA  SORTOP 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: MORSELESS 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

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>VALUE</th>
<th>NAME</th>
<th>THREAT</th>
<th>VALUE</th>
<th>NAME</th>
<th>FEATURES</th>
<th>VALUE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11</td>
<td>CENTRAL MACHINE</td>
<td>VERY HIGH</td>
<td>8</td>
<td>UNAUTHORIZED USE</td>
<td>MEDIUM</td>
<td>2</td>
<td>GUARD</td>
</tr>
<tr>
<td>2</td>
<td>11</td>
<td>CENTRAL MACHINE</td>
<td>VERY HIGH</td>
<td>10</td>
<td>HUMAN ERROR</td>
<td>PRETTY LOW</td>
<td>29</td>
<td>OPERATOR TRAINING</td>
</tr>
<tr>
<td>3</td>
<td>12</td>
<td>STORAGE MEDIA</td>
<td>HIGH</td>
<td>13</td>
<td>UNAUTHORIZED READ</td>
<td>HIGH</td>
<td>43</td>
<td>DATA ENCRYPTION</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td>STORAGE MEDIA</td>
<td>HIGH</td>
<td>15</td>
<td>THEFT</td>
<td>LOW</td>
<td>31</td>
<td>PHYSICAL ACCESS CONTROLS</td>
</tr>
<tr>
<td>5</td>
<td>71</td>
<td>METERING EQUIPMENT</td>
<td>LOW</td>
<td>4</td>
<td>HARDWARE TAMPERING—MODIFIED</td>
<td>LOW</td>
<td>21</td>
<td>LOCKS AND ALARMS ON MACHINE CO</td>
</tr>
<tr>
<td>6</td>
<td>23</td>
<td>DATA</td>
<td>HIGH</td>
<td>20</td>
<td>UNSECURED STORAGE MEDIA</td>
<td>HIGH</td>
<td>60</td>
<td>ADEQUATE AND ENFORCED LIBRARY</td>
</tr>
<tr>
<td>7</td>
<td>23</td>
<td>DATA</td>
<td>HIGH</td>
<td>33</td>
<td>EXPOSED OUTPUT</td>
<td>MEDIUM TO HIGH</td>
<td>61</td>
<td>USAGE LOG</td>
</tr>
<tr>
<td>8</td>
<td>23</td>
<td>DATA</td>
<td>HIGH</td>
<td>43</td>
<td>DATA PREPARATION ERRORS</td>
<td>PRETTY HIGH</td>
<td>90</td>
<td>CLEAN DESK POLICY</td>
</tr>
<tr>
<td>9</td>
<td>21</td>
<td>OPERATING SYSTEM</td>
<td>PRETTY HIGH</td>
<td>17</td>
<td>MODIFICATION OF OP SYS AND ROU</td>
<td>MEDIUM</td>
<td>103</td>
<td>SECOND PERSON VERIFICATION</td>
</tr>
</tbody>
</table>

Figure 4.1g Another data display
**Figure 4.1h  Continued use of the security evaluation functions**

<table>
<thead>
<tr>
<th>NAME</th>
<th>RATING (USING FUZZY MEAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATING SYSTEM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>DATA</td>
<td>SORTOF HIGH</td>
</tr>
<tr>
<td>THE LOWEST RATING WAS GIVEN TO:</td>
<td>OPERATING SYSTEM</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>NAME</th>
<th>RATING (USING FUZZY MEAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HARDWARE</td>
<td>((SLIGHTLY LOWER ) THAN FAIRLY HIGH )AND (SLIGHTLY HIGHER ) THAN SORTOF HIGH</td>
</tr>
<tr>
<td>SOFTWARE</td>
<td>((SLIGHTLY LOWER ) THAN SORTOF HIGH )AND (SLIGHTLY HIGHER ) THAN EXTREMELY MEDIUM</td>
</tr>
<tr>
<td>THE LOWEST RATING WAS GIVEN TO:</td>
<td>SOFTWARE</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>NAME</th>
<th>RATING (USING FUZZY MEAN WITH EACH MAJOR SUBSECTION WEIGHTED BY MAXIMUM OBJECT VALUE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HARDWARE</td>
<td>SORTOF HIGH</td>
</tr>
<tr>
<td>SOFTWARE</td>
<td>WORKORLESS MEDIUM</td>
</tr>
<tr>
<td>THE LOWEST RATING WAS GIVEN TO:</td>
<td>SOFTWARE</td>
</tr>
</tbody>
</table>
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.

**INDIVIDUAERATING (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 ①. 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 ②. 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 ③. 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 ④. 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 (6). 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 by 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) (3).

DELTRIP—this function deletes an existing triple (see also SAVE) (5).

MODTRIP—this function allows the user to modify existing triples (see also SAVE) (8).

SAVE—this function saves all of the user’s data in the user’s workspace (6). 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 PUNCH 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
      15 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


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 descending 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

A. Unauthorized access: R/W/E - F2.1, F2.2
16) Modification of operating system and system routines
17) Inadequate controls on I/O facilities - F2.3, F2.4
18) Password compromise - F2.5, F2.6, F2.7, F2.8
19) Unsecured storage medium - F2.9, F2.10, F2.11, F2.12
20) Access outside of allocated memory - F2.13, F2.14, F2.15
21) Modification of stored state vector - F2.16
22) Unauthorized CE activity
23) Line tapping and spoofing
24) Erroneous or inadequate usage of protection facilities - F2.17, F2.18, F2.19

B. Unauthorized access: read
26) Extra copies of output printed
27) duplicates printed
28) printing restarted before end
29) Use of erroneous distribution labels
30) Use of erroneous distribution lists
31) Theft of mail
32) Exposed output - F2.20, F2.21
33) in user possession
34) within distribution system
35) at operator's console
36) work in progress
37) Unauthorized reading of terminal buffers
38) Indirect exposure of output - F2.22, F2.23

C. Unauthorized access: write
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
50) 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


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
<table>
<thead>
<tr>
<th>Feature No</th>
<th>Threat No.</th>
<th>Feature Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Physical Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guard</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>ID Card Door</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Proper Location of Center</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Secure Door and Window Locks</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Personal Searches</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Two Operator System</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>Entrance Log</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>Outside Lighting</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>Fence</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>Alarm System</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>Closed Circuit TV</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>ID Badges</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>Secure Doors and Windows</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>Adequate Maintenance</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>Error Correcting Codes</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>Internal Machine Checks</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>Redundant Processors</td>
</tr>
<tr>
<td>19</td>
<td>3 4 5 6</td>
<td>The same features as Threat No. 1</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>Supervision and Authentication of CP's Locks and Alarms on Machine Covers</td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>7</td>
<td>The same features as Threat No. 1</td>
</tr>
<tr>
<td>23</td>
<td>8</td>
<td>Automatic Log</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>Locks on Controls</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td>Additionally, the same features as Threat No. 1</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>Status Indicators</td>
</tr>
<tr>
<td>27</td>
<td></td>
<td>Automatic Log</td>
</tr>
<tr>
<td>28</td>
<td>10</td>
<td>Proper Labelling</td>
</tr>
<tr>
<td>29</td>
<td></td>
<td>Operator Training</td>
</tr>
<tr>
<td>30</td>
<td></td>
<td>Detailed, accurate, accessible documentation</td>
</tr>
<tr>
<td>31</td>
<td>11</td>
<td>Physical Access Controls</td>
</tr>
<tr>
<td>32</td>
<td></td>
<td>Package and Briefcase Inspection</td>
</tr>
<tr>
<td>33</td>
<td></td>
<td>Gate-Pass System</td>
</tr>
<tr>
<td>34</td>
<td></td>
<td>Secure Library Facility</td>
</tr>
<tr>
<td>35</td>
<td></td>
<td>Proper Labelling</td>
</tr>
<tr>
<td>36</td>
<td>12</td>
<td>Control Checks</td>
</tr>
<tr>
<td>37</td>
<td></td>
<td>Checksum on Data</td>
</tr>
<tr>
<td>38</td>
<td></td>
<td>Effective Storage Access Controls</td>
</tr>
<tr>
<td>39</td>
<td></td>
<td>Header Checking</td>
</tr>
<tr>
<td>40</td>
<td></td>
<td>Preventive Measures</td>
</tr>
<tr>
<td>41</td>
<td></td>
<td>Write-Inhibit Switches</td>
</tr>
<tr>
<td>42</td>
<td></td>
<td>Ring Out for Tapes</td>
</tr>
<tr>
<td>43</td>
<td>13</td>
<td>Data Encryption</td>
</tr>
<tr>
<td>44</td>
<td></td>
<td>Effective Storage Access Controls</td>
</tr>
<tr>
<td>45</td>
<td>14 15</td>
<td>The same features as Threats 1-13</td>
</tr>
<tr>
<td>46</td>
<td>16</td>
<td>Effective Authorization and Access Control Mechanism</td>
</tr>
</tbody>
</table>
EFFECTIVE AUTHORIZATION AND ACCESS CONTROL MECHANISM

MINIMUM AUTHORIZATION POLICY

SUPER USER AUTHORIZATION REQUIRED FOR CHANGES

LOG OF ATTEMPTED VIOLATIONS

SELF-MODIFYING I/O ROUTINES NOT ALLOWED

DIRECTION IN PASSWORD CHOICE

STORE IN ENCRYPTED FORM

AUTOMATIC DELAY AFTER INVALID LOGIN ATTEMPT

ENCRYPTED TRANSMISSIONS TO TERMINALS

USY OF INTERACTIVE AUTHENTICATION PROCEDURE

Adequate access controls

Adequate and enforced library facility

Usage log

Proper labelling

Proper system design

Effective authorization and access control mechanism

Adequate I/O controls

Protection of state vector

Storage in protected storage

Administrative controls

Human verification

Supervision

Limited CE access

Encryption

Effective human engineering

Clear, easy to use protection facilities

Adequate documentation

User education

<See features for threats 27-39>

Print log

Security conscious I/O routines

Print log

Security conscious I/O routines

Careful administrative procedures

Careful administrative procedures

Important mail sent registered or by courier

Delivery confirmation

Track log of sensitive output

Library facility for sensitive output

<See also features for threats 34-37>

Clear desk policy

User education

Guarding work in transit
GUARDING WORK IN PROGRESS

BUFFER BRUSH MECHANISM

PAPER SHREDDER

USE OF OLD RIBBONS FOR SENSITIVE JOBS

DESTRUCTION OF CARBON PAPER AND RIBBONS

<REFER TO FEATURES FOR THREATS 41-44>

CAREFUL ADMINISTRATIVE PROCEDURES

IMPORTANT MAIL SENT REGISTERED OR BY COURIER

DELIVERY CONFIRMATION

SECOND PERSON VERIFICATION

CHECKSUMS

SOFTWARE CHECKS

VERIFICATION CHECKS

CHECKSUMS

SOFTWARE CHECKS

ORIGINATOR VERIFICATION

TESTING

AUDIT PROGRAMS

TESTING AND VERIFICATION

PENETRATION ATTEMPTS

PROGRAM TESTING AND VALIDATION

ADEQUATE DOCUMENTATION AND DESIGN SPECS

PROGRAM TESTING AND VALIDATION

PROGRAMMER EDUCATION

PROGRAM TESTING AND VALIDATION

CODE INSPECTION, RECOMPIRATION

CHOOSING WRITER WHO COULD NOT BENEFIT

TESTING ON SETUP DATA

CONTAINMENT OF TEST PROGRAMS

<REFER TO FEATURES FOR THREATS 54-56>

FIRE EXTINGUISHING SYSTEM

HEAT/SMOKE/FIRE DETECTORS WITH ALARMS

FIRE EXTINGUISHERS

AUTOMATIC EXTINGUISHING SYSTEM

FIRE PROTECTION MEASURES

FIREWALLS

FIREPROOF VAULT

FIRE DRILLS

FIRE PREVENTION MEASURES

NO SMOKING POLICY

USE OF FIRE RESISTANT MATERIALS

FLOOD PREVENTION MEASURES

ADEQUATE DRAINAGE

WATER SHUTOFF VALVE

WATER PROOF MACHINE COVERS

LOCATION NOT FLOOD-PRONE

COMPUTER ROOM NOT LOCATED IN THE BASEMENT

WATER PIPES NOT LOCATED DIRECTLY ABOVE THE EQUIPMENT
LOCATION NOT ON ACTIVE FAULT
ADEQUATE STRUCTURAL RE-ENFORCEMENT

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

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

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

<REFER TO FEATURES FOR THREAT NO. 57>

MONITORING EQUIPMENT AND ALARM SYSTEM

PREVENTIVE MAINTENANCE
HARDWARE CHECKS

ADEQUATE ADMINISTRATIVE PROCEDURES
BACKUP FACILITIES

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

POWER SUPPLY LINE FILTER
VOLTAGE STABILIZER FOR POWER SUPPLY
MONITORING SYSTEM WITH ALARM

ELECTRICAL INSPECTION

AUXILIARY WATER SUPPLY
FLOW MONITOR WITH ALARM

WATER FILTERS

TEMPERATURE CONTROLLERS
TEMPERATURE MONITOR WITH ALARM

EMERGENCY LIGHTS
AUXILIARY POWER SUPPLY

ALARM SYSTEM
CONTINGENCY PLANS

<REFEER TO FEATURES FOR THREAT NO. 54>

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

<REFER TO FEATURES FOR THREAT NO. 56>

<REFER TO FEATURES FOR THREAT NO. 57>

<REFER TO FEATURES FOR THREAT NO. 58>

<REFER TO FEATURES FOR THREAT NO. 59>

<REFER TO FEATURES FOR THREAT NO. 60>

<REFER TO FEATURES FOR THREAT NO. 61>

PROPER PHYSICAL AREA DESIGN AND CONSTRUCTION

BACKUP COMMUNICATIONS EQUIPMENT
ELECTRICAL SHIELDING
ELECTRICAL SHIELDING OF OPERATIONS AREA
STORAGE OF MAGNETIC MEDIA IN SHIELDING SAFES

SECURE LIBRARY Facilities
SECURE TAPE AND DISK LIBRARY
ONLY AUTHORIZED PERSONNEL ALLOWED TO ENTER LIBRARY

PAPER SHREDDER
USE OF OLD RIBBONS WITH SENSITIVE JOBS
INCINERATORS
EMPLOYEE AWARENESS AND EDUCATION
SECURE DISPOSAL BINS

REASONABLE AND INDUSTRY COMPARABLE SALARIES
REFERENCE CHECKING
CAREFUL SUPERVISION

REASONABLE AND INDUSTRY COMPARABLE SALARIES
REFERENCE CHECKING
CAREFUL SUPERVISION
EMPLOYEE MORALE PROGRAMS

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

IMMEDIATE NOTICE ON LAYOFF (WITH APPROPRIATE PAY)
PROMPT EMPLOYEE COMPLAINT HANDLING
<REFE ALSO TO FEATURES FOR THREAT NO. 92>

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

REFERENCE CHECKING
LIMIT EMPLOYEE AUTHORITY
NEED TO KNOW POLICY

REFERENCE CHECKING
CORPORATE INTELLIGENCE

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

USE LOG
LIBRARY STORAGE

USE LOG
LIBRARY STORAGE
CLEAN DESK POLICY
CLEARLY DEFINED AUTHORIZATION FOR MODIFICATION
CLEAR CLASSIFICATION LABELLING
CLEAN DESK POLICY
USE LOG
PROTECTED LIBRARY STORAGE
GOOD COMMUNICATION SYSTEM BETWEEN THE SITES
SIMULATED DISASTER TESTS
RECIPIROCAL AGREEMENTS BETWEEN COMPANIES (INCLUDES PERSONNEL)
USE OF SIMILAR EQUIPMENT FOR BACKUP (WITH PERIODIC RECHECKING)
ADEQUATE EMPLOYEE TRAINING
SIMULATED DISASTER TESTS
(ALSO REFER TO THE SECTION ON HARDWARE)
SIMULATED DISASTER TESTS
PROGRAM FOR BACKUP MAINTENANCE
ADEQUATE EMPLOYEE TRAINING
SIMULATED DISASTER TESTS
DUPLICATE DATA STORED SAFELY
SIMULATED DISASTER TESTS
(SEE ALSO SECTION ON SOFTWARE)
BACKUP GENERATOR AND FUEL
BACKUP STORE OF FUEL
BACKUP STORE OF OPERATIONS MATERIALS
(SEE ALSO SECTION ON THE COMPUTER CENTER)
PROPER PLANNING
SIMULATED DISASTER TESTS
CONTINGENCY PLANS FOR REACHING PERSONNEL AWAY FROM WORK
SIMULATED DISASTER TESTS
PROPER PLANNING
SIMULATED DISASTER TESTS
PROGRAM FOR BACKUP MAINTENANCE
SIMULATED DISASTER TESTS
PROPER PLANNING
SIMULATED DISASTER TESTS
PROGRAM FOR BACKUP MAINTENANCE
SIMULATED DISASTER TESTS
PROPER PLANNING
ADEQUATE EMPLOYEE TRAINING
SIMULATED DISASTER TESTS
(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
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 reinforcement) #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
<table>
<thead>
<tr>
<th>OBJECT NO:</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ADD, A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VALUE, V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT NO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT LIKELIHOOD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FEATURE NOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FEATURE RESISTANCE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECT NO:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADD, A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VALUE, V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT NO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT LIKELIHOOD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FEATURE NOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FEATURE RESISTANCE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECT NO:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADD, A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VALUE, V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT NO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT LIKELIHOOD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FEATURE NOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FEATURE RESISTANCE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECT NO:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADD, A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VALUE, V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT NO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT LIKELIHOOD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FEATURE NOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FEATURE RESISTANCE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECT NO:</td>
<td>A METERING EQUIPMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADD, A name or number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VALUE, V object value</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT NO</td>
<td>THREAT LIKELIHOOD</td>
<td>FEATURE NOS</td>
<td>FEATURE RESISTANCE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>MEDIUM</td>
<td>2</td>
<td>PRETTY HIGH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>MEDIUM LOW</td>
<td>2.9</td>
<td>PRETTY HIGH</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECT NO:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADD, A name or number</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VALUE, V object value</td>
<td>V HIGH</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT NO</td>
<td>THREAT LIKELIHOOD</td>
<td>FEATURE NOS</td>
<td>FEATURE RESISTANCE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>HIGH</td>
<td>43 44</td>
<td>PRETTY HIGH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>LOW</td>
<td>31</td>
<td>PRETTY HIGH</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECT NO:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADD, A name or number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VALUE, V object value</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT NO</td>
<td>THREAT LIKELIHOOD</td>
<td>FEATURE NOS</td>
<td>FEATURE RESISTANCE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>LOW</td>
<td>21</td>
<td>HIGH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECT NO:</td>
<td>ADD, A name or number</td>
<td>VALUE, V object value</td>
<td>THREAT NO</td>
<td>THREAT LIKELIHOOD</td>
<td>FEATURE NOS</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------</td>
<td>----------------------</td>
<td>-----------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>16</td>
<td>104</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBJECT NO:</th>
<th>ADD, A name or number</th>
<th>VALUE, V object value</th>
<th>THREAT NO</th>
<th>THREAT LIKELIHOOD</th>
<th>FEATURE NOS</th>
<th>FEATURE RESISTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td></td>
<td></td>
<td>45</td>
<td>FAIRLY HIGH</td>
<td>114</td>
<td>MEDIUM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBJECT NO:</th>
<th>ADD, A name or number</th>
<th>VALUE, V object value</th>
<th>THREAT NO</th>
<th>THREAT LIKELIHOOD</th>
<th>FEATURE NOS</th>
<th>FEATURE RESISTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2</td>
<td></td>
<td></td>
<td>46</td>
<td>FAIRLY HIGH</td>
<td>114</td>
<td>FAIRY LOW TO MEDIUM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBJECT NO:</th>
<th>ADD, A name or number</th>
<th>VALUE, V object value</th>
<th>THREAT NO</th>
<th>THREAT LIKELIHOOD</th>
<th>FEATURE NOS</th>
<th>FEATURE RESISTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3</td>
<td></td>
<td></td>
<td>2.0</td>
<td>HIGH</td>
<td>60 61</td>
<td>PRETTY LOW</td>
</tr>
<tr>
<td>3.3</td>
<td></td>
<td></td>
<td>3.3</td>
<td>MEDIUM TO HIGH</td>
<td>92 94</td>
<td>LOW</td>
</tr>
<tr>
<td>4.3</td>
<td></td>
<td></td>
<td>4.3</td>
<td>PRETTY HIGH</td>
<td>105 104 105</td>
<td>HIGH</td>
</tr>
<tr>
<td>OBJECT NO:</td>
<td>23</td>
<td>23</td>
<td>31</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADD, A name or number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VALUE, V object value</td>
<td>V (FAIRLY HIGH) TO HIGH</td>
<td>V (FAIRLY HIGH) TO HIGH</td>
<td>V VERY HIGH</td>
<td>V MEDIUM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>THREAT NO</td>
<td>THREAT LIKELIHOOD</td>
<td>FEATURE NOS</td>
<td>FEATURE RESISTANCE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
<td>-------------</td>
<td>-------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>SORT OF LOW</td>
<td>0</td>
<td>LOW TO MEDIUM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>HIGH</td>
<td>0</td>
<td>LOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>FAIRLY LOW</td>
<td>114</td>
<td>LOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>FAIRLY LOW</td>
<td>136 127</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>FAIRLY LOW</td>
<td>126 127</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECT NO:</td>
<td>ADD, A name or number</td>
<td>VALUE, V object value</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------</td>
<td>-----------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>THREAT NO</th>
<th>THREAT LIKELIHOOD</th>
<th>FEATURE NOS</th>
<th>FEATURE RESISTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>84</td>
<td>LOW</td>
<td>2</td>
<td>PRETTY HIGH</td>
</tr>
<tr>
<td>86</td>
<td>MEDIUM</td>
<td>2, 11</td>
<td>PRETTY HIGH</td>
</tr>
</tbody>
</table>
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:

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

Object no 11, central machine is next.

Very high

Threat no threat likelihood feature nos feature resistance

+ 6 medium 2 pretty high

+ 10 pretty low 29 30 medium

+ N

Object no 12, storage media is next.

Very 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.

Very low

Threat no threat likelihood feature nos feature resistance

+ 4 low 21 high

+ N

Enter the object number for the next object: 2

Software:

Very high

Threat no threat likelihood feature nos feature resistance

+ 16 medium 46 medium to pretty high

+ 0

Object no 21, operating system is next.

V high
OBJECT NO 22, PROGRAMS IS NEXT.
: V MEDIUM

OBJECT NO 23, DATA IS NEXT.
: V HIGH

OBJECT NO 231, PERSONAL DATA IS NEXT.
: N

OBJECT NO 232, INSTITUTION DATA IS NEXT.
: V (FAIRLY HIGH) TO HIGH

OBJECT NO 2321, MARKETING DATA IS NEXT.
: N

OBJECT NO 2322, FINANCIAL DATA IS NEXT.
: V (FAIRLY HIGH) TO HIGH

OBJECT NO 2323, OPERATIONS DATA IS NEXT.
: N

OBJECT NO 2324, PLANNING DATA IS NEXT.
: N

OBJECT NO 2325, OTHER DATA IS NEXT.
: N

OBJECT NO 31, RESOURCE SUPPLY SYSTEMS IS NEXT.
: V VERY HIGH

OBJECT NO 32, THE BUILDING IS NEXT.
: V MEDIUM

OBJECT NO 321, THE BUILDING STRUCTURE IS NEXT.
: N
Following is a list of objects added, their assigned object numbers, and their parent in the hierarchy:

<table>
<thead>
<tr>
<th>Objects</th>
<th>Threats</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triple * Number</td>
<td>Name * Value</td>
<td>Number * Name * Likelihood</td>
</tr>
<tr>
<td>1</td>
<td>11 CENTRAL MACHINE * VERY HIGH</td>
<td>8 UNAUTHORIZED USE * MEDIUM</td>
</tr>
<tr>
<td>2</td>
<td>11 CENTRAL MACHINE * VERY HIGH</td>
<td>10 HUMAN ERROR * PRETTY LOW</td>
</tr>
<tr>
<td>3</td>
<td>12 STORAGE MEDIA * HIGH</td>
<td>13 UNAUTHORIZED READ * HIGH</td>
</tr>
<tr>
<td>4</td>
<td>12 STORAGE MEDIA * HIGH</td>
<td>11 THEFT * LOW</td>
</tr>
<tr>
<td>5</td>
<td>71 METERING EQUIPMENT * LOW</td>
<td>4 HARDWARE TAMPERING--MODIFIED</td>
</tr>
<tr>
<td>6</td>
<td>2 SOFTWARE * VERY HIGH</td>
<td>16 UNAUTHORIZED ACCESS--R/W/E</td>
</tr>
<tr>
<td>7</td>
<td>21 OPERATING SYSTEM * HIGH</td>
<td>45 DEFECTIVE IMPLEMENTATION</td>
</tr>
<tr>
<td>8</td>
<td>22 PROGRAMS * MEDIUM</td>
<td>46 INADEQUATE DEBUGGING</td>
</tr>
<tr>
<td>9</td>
<td>23 DATA * HIGH</td>
<td>20 UNSECURED STORAGE MEDIA</td>
</tr>
<tr>
<td>10</td>
<td>23 DATA * HIGH</td>
<td>33 EXPOSED OUTPUT</td>
</tr>
<tr>
<td>11</td>
<td>23 DATA * HIGH</td>
<td>43 DATA PREPARATION ERRORS</td>
</tr>
<tr>
<td>12</td>
<td>232 INSTITUTION DATA * FAIRLY HIGH TO HIGH</td>
<td>0 SORTOF LOW</td>
</tr>
<tr>
<td>13</td>
<td>2322 FINANCIAL DATA * FAIRLY HIGH TO HIGH</td>
<td>0 HIGH</td>
</tr>
<tr>
<td>14</td>
<td>31 RESOURCE SUPPLY SYSTEMS * VERY HIGH</td>
<td>56 EARTHQUAKE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
OBJECT NO 322, COMPUTER OPERATIONS AREA IS NEXT.
: O
OBJECT NO 3221, COMPUTER ROOM IS NEXT.
: V HIGH
THREAT NO THREAT LIKELIHOOD FEATURE NO. FEATURE RESISTANCE
+ 54 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 I RATE)

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
<table>
<thead>
<tr>
<th>Location</th>
<th>Category</th>
<th>Risk 1</th>
<th>Risk 2</th>
<th>Risk 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 RESOURCE SUPPLY SYSTEMS</td>
<td>* 54 FIRE</td>
<td>FAIRLY LOW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>* 54 FIRE</td>
<td></td>
<td>FAIRLY LOW</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>* 54 FIRE</td>
<td></td>
<td></td>
<td>MEDIUM</td>
</tr>
<tr>
<td>16 THE BUILDING</td>
<td>* 73 FIRE</td>
<td>FAIRLY LOW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>* 73 FIRE</td>
<td></td>
<td>FAIRLY LOW</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>* 73 FIRE</td>
<td></td>
<td></td>
<td>MEDIUM</td>
</tr>
<tr>
<td>16</td>
<td>* 73 FIRE</td>
<td></td>
<td></td>
<td>MEDIUM</td>
</tr>
<tr>
<td>17 COMPUTER ROOM</td>
<td>* 84 MAGNETS</td>
<td>LOW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>* 84 MAGNETS</td>
<td></td>
<td>LOW</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>* 84 MAGNETS</td>
<td></td>
<td></td>
<td>MEDIUM</td>
</tr>
<tr>
<td>18 COMPUTER ROOM</td>
<td>* 86 UNAUTHORIZED INTRUDERS</td>
<td>MEDIUM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>* 86 UNAUTHORIZED INTRUDERS</td>
<td></td>
<td>MEDIUM</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>* 86 UNAUTHORIZED INTRUDERS</td>
<td></td>
<td></td>
<td>MEDIUM</td>
</tr>
<tr>
<td>126 HEAT/SMOKE/FIRE DETECTORS WITH FIRE EXTINGUISHERS</td>
<td>* 127 FIRE EXTINGUISHERS</td>
<td>MEDIUM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>* 127 FIRE EXTINGUISHERS</td>
<td></td>
<td>MEDIUM</td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>* 127 FIRE EXTINGUISHERS</td>
<td></td>
<td></td>
<td>MEDIUM</td>
</tr>
<tr>
<td>126</td>
<td>* 126 HEAT/SMOKE/FIRE DETECTORS WITH FIRE EXTINGUISHERS</td>
<td></td>
<td></td>
<td>MEDIUM</td>
</tr>
<tr>
<td>126</td>
<td>* 126 HEAT/SMOKE/FIRE DETECTORS WITH FIRE EXTINGUISHERS</td>
<td></td>
<td></td>
<td>MEDIUM</td>
</tr>
<tr>
<td>2 GUARD</td>
<td>(PRETTY LOW) TO MEDIUM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 GUARD</td>
<td>(PRETTY LOW) TO MEDIUM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 ALARM SYSTEM</td>
<td>PRETTY HIGH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 ALARM SYSTEM</td>
<td>PRETTY HIGH</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DO YOU WANT TO SEE A DESCRIPTION OF THE RATING FUNCTIONS? Y

THE FOLLOWING RATING FUNCTIONS ARE AVAILABLE:
1) WEAKEST LINK
2) SELECTED WEAKST 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
OVERALL RATING

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

DO YOU WANT TO SEE A DESCRIPTION OF THE RATING FUNCTIONS? N
ENTER THE NUMBER OF THE RATING FUNCTION YOU WISH TO USE: 2
SECTIONAL RATING

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
********************************************************************************

SET RATE 1

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
OPERATING SYSTEM
PROGRAMS
DATA

RATING (USING FUZZY MEAN WEIGHTED BY VALUE)
MORGERS MEDIUM) TO (SORT OF HIGH)

THE LOWEST RATING WAS GIVEN TO:...
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 LIKELIHOOD
6) FEATURE RESISTANCE

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
METERING EQUIPMENT 71

<table>
<thead>
<tr>
<th>OBJECTS</th>
<th>NUMBERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>VALUE</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>11</td>
<td>CENTRAL MACHINE</td>
</tr>
<tr>
<td>11</td>
<td>CENTRAL MACHINE</td>
</tr>
<tr>
<td>12</td>
<td>STORAGE MEDIA</td>
</tr>
<tr>
<td>12</td>
<td>STORAGE MEDIA</td>
</tr>
<tr>
<td>71</td>
<td>METERING EQUIPMENT</td>
</tr>
<tr>
<td>2</td>
<td>SOFTWARE</td>
</tr>
<tr>
<td>21</td>
<td>OPERATING SYSTEM</td>
</tr>
<tr>
<td>22</td>
<td>PROGRAMS</td>
</tr>
<tr>
<td>23</td>
<td>DATA</td>
</tr>
<tr>
<td>23</td>
<td>DATA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>THREATS</th>
<th>NUMBERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>LIKELIHOOD</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>8</td>
<td>UNAUTHORIZED USE</td>
</tr>
<tr>
<td>10</td>
<td>HUMAN ERROR</td>
</tr>
<tr>
<td>13</td>
<td>UNAUTHORIZED READ</td>
</tr>
<tr>
<td>11</td>
<td>THEFT</td>
</tr>
<tr>
<td>16</td>
<td>UNAUTHORIZED ACCESS--R/W/E</td>
</tr>
<tr>
<td>45</td>
<td>DEFECTIVE IMPLEMENTATION</td>
</tr>
<tr>
<td>46</td>
<td>INADEQUATE DEBUGGING</td>
</tr>
<tr>
<td>20</td>
<td>UNSECURED STORAGE MEDIA</td>
</tr>
<tr>
<td>33</td>
<td>EXPOSED OUTPUT</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>NUMBERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>RESISTANCE</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>2</td>
<td>GUARD</td>
</tr>
<tr>
<td>29</td>
<td>OPERATOR TRAINING</td>
</tr>
<tr>
<td>30</td>
<td>DETAILED, ACCURATE, ACCESSIBLE</td>
</tr>
<tr>
<td>43</td>
<td>DATA ENCRYPTION</td>
</tr>
<tr>
<td>44</td>
<td>EFFECTIVE STORAGE ACCESS CONTROL</td>
</tr>
<tr>
<td>31</td>
<td>PHYSICAL ACCESS CONTROLS</td>
</tr>
<tr>
<td>21</td>
<td>LOCKS AND ALARMS ON MACHINE CONTROL</td>
</tr>
<tr>
<td>46</td>
<td>EFFECTIVE AUTHORIZATION AND ACCESS CONTROL</td>
</tr>
<tr>
<td>112</td>
<td>TESTING AND VERIFICATION</td>
</tr>
<tr>
<td>114</td>
<td>PROGRAM TESTING AND VALIDATION</td>
</tr>
<tr>
<td>60</td>
<td>ADEQUATE AND ENFORCED LIBRARY ACCESS</td>
</tr>
<tr>
<td>90</td>
<td>CLEAN DESK POLICY</td>
</tr>
<tr>
<td>91</td>
<td>USER EDUCATION</td>
</tr>
</tbody>
</table>
**INSTITUTION DATA**
- Very High
- High

**FINANCIAL DATA**
- Fairly High to High

**RESOURCE SUPPLY SYSTEMS**
- Very High

**THE BUILDING**
- Medium

**COMPUTER ROOM**
- High
- Medium

**DATA PREPARATION ERRORS**
- Pretty High

**SECOND PERSON VERIFICATION**
- Low

**CHECKSUMS**
- Low to Medium

**SOFTWARE CHECKS**
- High

**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 Likelihood
  6. Feature Resistance

* Enter the new feature resistance: Medium
**WRATE**

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

<table>
<thead>
<tr>
<th>NAME</th>
<th>RATING (USING FUZZY MEAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATING SYSTEM</td>
<td>MOREORLESS MEDIUM</td>
</tr>
<tr>
<td>PROGRAMS</td>
<td>MOREORLESS MEDIUM</td>
</tr>
<tr>
<td>DATA</td>
<td>MEDIUM</td>
</tr>
</tbody>
</table>

*THE LOWEST RATING WAS GIVEN TO:*
*OPERATING SYSTEM*
*PROGRAMS*
Appendix C

Formal Language Definition

\[\text{sentence} ::= \text{compound phrase} \mid \text{simple phrase}\]
\[\text{compound phrase} ::= \text{conjunctive phrase} \mid \text{range phrase}\]
\[\text{simple phrase} ::= \text{relational phrase} \mid \text{hedged primary}\]
\[\text{conjunctive phrase} ::= \text{relational phrase} \text{ AND relational phrase}\]
\[\text{range phrase} ::= \text{hedged primary} \text{ TO hedged primary}\]
\[\text{relational phrase} ::= \text{composite relation} \text{ THAN hedged primary}\]
\[\text{composite relation} ::= \text{relation hedge} \text{ relation} \mid \text{relation}\]
\[\text{relation hedge} ::= \text{NOT} \mid \text{MUCH} \mid \text{SLIGHTLY}\]
\[\text{relation} ::= \text{LOWER} \mid \text{HIGHER}\]
\[\text{hedged primary} ::= \text{hedge} \text{ primary} \mid \text{primary} \mid \text{fuzzy number}\]
\[\text{hedge} ::= \text{NOT} \mid \text{VERY} \mid \text{MORE OR LESS} \mid \text{QUITE} \mid \text{PRETTY} \mid \text{SORT OF} \mid \text{REALLY} \mid \text{EXTREMELY} \mid \text{INDEED}\]
\[\text{primary} ::= \text{LOW} \mid \text{HIGH} \mid \text{MEDIUM}\]
\[\text{fuzzy number} ::= \text{fuzzifier} \text{ number}\]
\[\text{fuzzifier} ::= \text{ABOUT}\]
\[\text{number} ::= 1 \mid 2 \mid 3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9 \mid 10\]

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

- high
- low
- medium
- not high
- more or less 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 sort of 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 AF.

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 relevant 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

<table>
<thead>
<tr>
<th>Primary Terms</th>
<th>Primary Hedges</th>
<th>Relations</th>
</tr>
</thead>
<tbody>
<tr>
<td>high</td>
<td>extremely</td>
<td>lower than</td>
</tr>
<tr>
<td>low</td>
<td>very</td>
<td>higher than</td>
</tr>
<tr>
<td>medium</td>
<td>pretty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>fairly</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sortof</td>
<td></td>
</tr>
<tr>
<td>Relation Hedges</td>
<td>Connectives</td>
<td></td>
</tr>
<tr>
<td>not</td>
<td>and</td>
<td></td>
</tr>
<tr>
<td>much</td>
<td>to</td>
<td></td>
</tr>
<tr>
<td>slightly</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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