A PRACTICAL FRAMEWORK
FOR COMPUTER INSTALLATION SECURITY

by

Eric Michelman

Memorandum No. UCB/ERL M77/4

31 May 1977

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

A PRACTICAL FRAMEWORK
FOR COMPUTER INSTALLATION SECURITY*

Eric Michelman

Computer Science Division
Department of Electrical Engineering and Computer Sciences
and the Electronics Research Laboratory
University of California, Berkeley

Abstract

A security oriented model of a computer installation is presented along the lines of Clements' object-threat-feature conceptualization [1]. He suggests modelling a computer installation in terms of a set of objects, one or more threats per object, and a security feature for each object-threat pair. The model presented here considers objects and threats but not measures. Another category, flaws, is introduced as a characteristic of a computer system which increases the likelihood of a threat succeeding.

An enumeration of objects commonly found in a commercial installation is arranged hierarchically. The corresponding threats and flaws are then listed separately under the same hierarchical structure.

*Research sponsored by National Science Foundation Grant MCS76-09214.

Introduction

This model is presented as a representation of a data processing installation, focusing on those features which are relevant to security. The bulk of the model is concerned with the actual computer system, however the physical and organizational aspects of an installation are also considered.

The purpose of this model is to provide a representation of a computer security system which is complete, clear, well-defined, and easy to work with. In particular, it was designed to be used in the evaluation of security systems, in conjunction with the work being done by Don Clements [1].

Model Description

The form of the model is based on the security system model proposed by Clements. His model has three components, objects, threats, and measures, plus connections between them. These components are defined as follows:

Object -- resource within a computing system, the loss of which would have a cost to the owner.

Threat -- activity which a potential intruder may employ to gain unauthorized access to an object. Also refers to chance

*Research sponsored by National Science Foundation Grant MCS76-09214.

events which may jeopardize an object.

Feature -- protective measure in a computing system which presents some degree of resistance to a penetration attempt (firewall function).

Clements illustrates the interrelationship between the objects, threats, and features with the figure below.

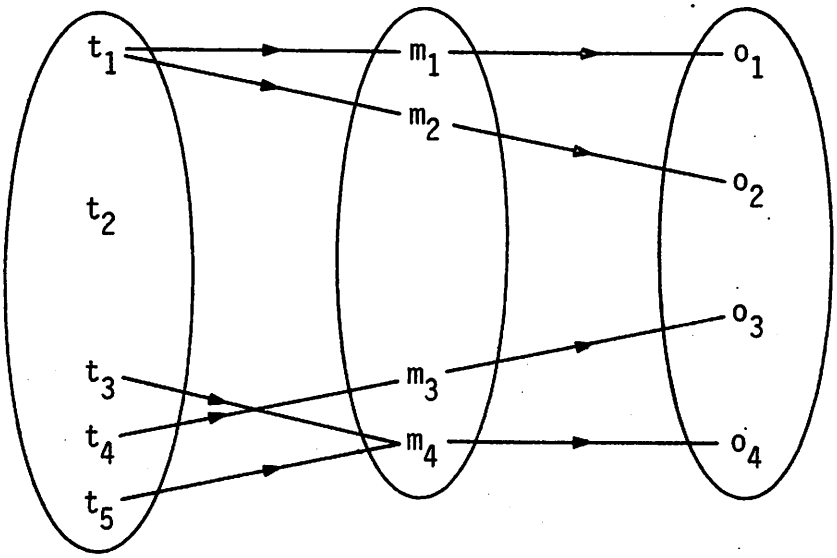

FIGURE 1. THE BASIC SECURITY SYSTEM

The model developed here appropriates the concepts of objects and threats and adds another component, flaws.

Flaw -- a characteristic of a computing system which enhances the likelihood of a threat succeeding in compromising an object.

Each flaw is associated with a particular threat, as shown in Figure 2. The purpose of the flaws category is to map what a user of a security evaluation system may perceive as threats into threats as viewed by the model. This is discussed more fully in the Development section.

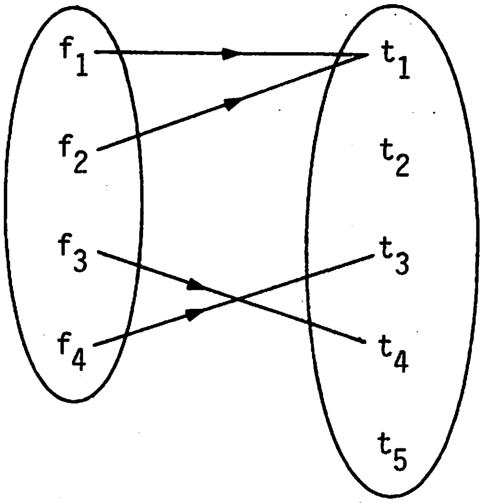

FIGURE 2. THE FLAW-THREAT RELATION

The structure of the model is centered around the object category, which is structured hierarchically. Associated with each object is a list of those threats which may affect that object. Associated with each threat is a list of those flaws which are related to that threat.

The hierarchical structuring of the objects was one of the primary goals of the project. It is the principal factor in keeping the model as clear and well defined as possible. For use within the evaluation system, it provides the following benefits:

a) Easier to understand -- The user is confronted with a logically structured model and a minimum of information is facing him at any one time.

b) Greater flexibility -- The user is able to restrict evaluation to only those areas of the computer installation which interest him. The inability to do this was a major criticism of a similar system when it was tested [2]. Related to the user's time saving is the cost savings in less computer time.

c) More informative results -- Each functional area of the computer installation can be rated separately. This would enable the user to more accurately determine which areas need the most attention. This could also be used as an iterative design aid for achieving a balanced security system with a limited security budget.

d) Expedite testing -- Testing could be made easier and shorter by considering only one subsection. At the same time the test ratings would refer to an identifiable subsection.

The objects, threats, and flaws were derived primarily from the 1974 AFIPS Security Review Manual [3] and the SAFE Audit Manual [4]; however other sources were also used [5,6,7,8,9,10].

The actual objects, threats, and flaws used, along with the actual structuring, were based primarily on these criteria:

a) Technical accuracy -- The technical aspects of the computer system must be accurately represented if a security rating is to be valid.

b) Based on previous work -- A primary objective was to develop the model along the lines of Clements' suggested model to facilitate its inclusion in the rating system.

c) Perceived system structure -- Within the limits of (a) and (b) the model was designed to coincide with an evaluation system user's perception of a computer system, thus providing greater ease of use and more accurate results.

Development

The greatest difference between the model produced and what was envisioned at the outset was the introduction of the flaws category.

As part of the object-threat-feature model of a computer security system, a flaws cateogry is unnecessary. That is, for the theoretical purposes of the model, it is complete without the extra category. However, upon creating a computer installation model along the lines of the object-threat-feature framework, it became clear that there were possible aspects of the system which, while not being threats according to the strict model definition, do seem to threaten security. A simple example of this would be leaving confidential material exposed. This would seem to be a threat to security, however the model takes the position that the security threat would be an unauthorized person viewing the exposed material. The problem with this is that an unauthorized person couldn't view the material if it weren't exposed. Clements' model accounts for that though, in the feature category, which in this case would be tighter controls on confidential material.

The point is that while the model may be logically complete, in this type of instance it doesn't always correspond to how a person would view a situation. Since the computer installation model was designed with a primary objective being its incorporation into a security evaluation system, it was felt that it was important for it to correspond to a user's view of an installation. To accomplish this and keep the theoretical basis for the system intact, a new category was formed, that of flaws. The function of the flaws category is to take what a user might think of as a security threat and map it into the corresponding threat according to the model. This is accomplished through the link between threats and flaws.

The benefits of this approach are expected to be better accuracy in actual use and greater user confidence in the security evaluation system.

Another question which needed to be resolved was whether or not objects such as personnel and the building were actually objects as defined in the model. The question was whether building actually has an intrinsic value to the computing system, or is just a practical necessity (consider an HP-65). Also, personnel are possibly either a practical convenience or a security feature, not an object. It was decided to include them as objects because in today's systems they are necessary for operation, both have a loss value, and both require protection against possible threats.

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

The 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
  - Malicious destruction - F1.1
  - Hardware error - F1.4
  - Hardware tampering - F1.1, F1.4, F1.5
    - modified operation
    - loss of data
    - modification of data
  - Tampering with panel controls
  - Unauthorized use - F1.2
  - Unauthorized change in operating characteristics during operation - F1.2
  - Human error - F1.6, F1.7
- 1.2 Storage media
  - Theft - F1.3
  - Unauthorized modification - F1.3
  - Unauthorized read - F1.3
- 1.3 Communications equipment
  - <same threats as 1.1 Central machine>
- 1.4 I/O devices
  - <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

      Modification of operating system and system routines

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

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

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

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

      Modification of stored state vector - F2.16

      Unauthorized CE activity

      Line tapping and spoofing

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

   B. Unauthorized access: read

      Extra copies of output printed

         duplicates printed

         printing restarted before end

      Use of erroneous distribution labels

      Use of erroneous distribution lists

      Theft of mail

      Exposed output - F2.20, F2.21

         in user possession

         within distribution system

         at operator's console

         work in progress

      Unauthorized reading of terminal buffers

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

   C. Unauthorized access: write

      Modification or spoof of mail transactions

      Unauthorized modification of data during preparation - F2.24

      Data preparation errors - F2.24

      Modification of original written data input - F2.25

2.1 Operating system

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

2.2 Programs

Inadequate debugging

Incomplete operation specifications

Inadequate or erroneous error handling

Exposure following abnormal end

Improper operation

2.2.2 Contract programs and packages

Dishonest programs

2.2.4 Test programs

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
     - Natural calamities
       - Fire
       - Flood
       - Earthquake
     - Manmade disasters
       - Smoke
       - Rioting
       - Bombing
       - Vandalism
     - Fate (chance events)
       - Equipment breakdown
       - Shutdown of building facilities
     - 3.1.2 Power
       - Blackout
       - Fluctuations
       - Grounding problems
     - 3.1.3 Water
       - Disruption
       - Contamination
       - Temperature variations
     - 3.1.4 Lighting
       - Blackout
   - 3.2 The Building
     - Natural calamities
       - Fire
       - Flood
       - Earthquake
     - Manmade disasters
       - Smoke
       - Rioting
       - Bombing
       - Vandalism

3.2.2 Computer operations area

Shocks and vibrations

Communications breakdown

Illegal entry and burglary

3.2.2.1 Computer room

Magnets

Electromagnetic radiation, to and from

3.2.2.2 Data reception

Unauthorized intruders

3.2.2.3 Tape and disk library

Magnets

3.2.2.6 Physical plant room

Sabotage

3.3 Waste materials

Unauthorized reading

Theft

4. Personnel
   - Bribery - F4.1
   - Dissatisfaction or malice - F4.1, F4.2
     - Towards the institution
     - Towards management
     - Towards other workers
     - Towards others (possibly unknown)
   - Greed - F4.1, F4.2
     - Competitor encouraged
     - Entrepreneurial tendencies
   - Incompetence - F4.1
   - Coercion - F4.1, F4.2
   - Competitor plants (industrial espionage)
   - Carelessness - F4.1

   Personnel Flaws
   - F4.1 Personal instability
   - F4.2 Job insecurity

5. Documentation

   Loss - F5.1, F5.2

   Thievery - F5.1, F5.2

   Unauthorized viewing - F5.1, F5.2

   Unauthorized modification - F5.1, F5.2

Documentation Flaws

F5.1 Inadequate signout procedures

F5.2 Documentation left unsecured

6. Backup system

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

6.1 Hardware

Incompatibility with other equipment in use

Ignorance of operation

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

6.2 Software

Not up to date

Incompatible system components

Ignorance of use

Lack of necessary data

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

6.3 The Computer Center

Malfunctioning power generation system

Shortage of generator fuel

Shortage of operation materials

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

6.4 Personnel

Lack of transportation to backup site

Lack of communication

6.5 Documentation, operational procedures

Inadequate communications facilities

Incompatible run procedures

Inadequate office, other operational facilities

Unplanned emergency run schedules

Inadequate personnel direction

Confusion during disaster - F6.6

<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

Summary

A hierarchical structuring of objects commonly found in a commercial computer installation was presented with a corresponding list of security threats.

This model was incorporated in a security evaluation and analysis system which has been implemented based on Clements' work. Both the input data and the analysis were structured along the lines of this hierarchy. The resultant system is now operable and has been tested on actual installations [11].

References

1. Lance J. Hoffman and Don Clements, "Fuzzy Computer Security Metrics: A Preliminary Report," Memorandum No. UCB/ERL M77/6, 27 January 1977, UCB-CS-76-42, Electronics Research Laboratory, College of Engineering, University of California, Berkeley.

2. Don Clements and Lance J. Hoffman, "Computer Assisted Security System Design," Memorandum No. ERL-M468, Electronics Research Laboratory, College of Engineering, University of California, Berkeley, November 1974.

3. AFIPS Systems Review Manual on Security, AFIPS, Montvale, N.J., 1974.

4. Leonard I. Krauss, Security Audit and Field Evaluation for Computer Facilities and Information Systems, Firebrand, Krauss and Co., P.O. Box 165, East Brunswick, N.J., 1972.

5. Farr, Chadwick, and Wong, Security for Computer Systems, National Computing Centre Limited, Manchester, England, 1972.

6. Wooldridge, Corder, and Johnson, Security Standards for Data Processing, Halsted Press, 1973.

7. Richard R. Linde, "Operating System Penetration," National Computer Conference, 1975, pp. 361-368.

8. Clark Weissman, "System Security Analysis/Certification Methodology and Results," System Development Corp., Memo #SP-3728, October 1973.

9. Lee Molho, "Hardware Aspects of Secure Computing," Spring Joint Computer Conference 1970, pp. 135-141.

10. IBM, "Data Security--Threats and Deficiencies in Computer Operations --A Report on a Completed Survey--A Translation from an IBM Svenska AB Publication (G320-5646)," 1975.

11. Eric Michelman, "A Security Evaluation and Analysis System," Memorandum No. UCB/ERL M77/36, Electronics Research Laboratory, College of Engineering, University of California, Berkeley