COMPUTER SECURITY AND PROTECTION STRUCTURES

Bruce J. Walker
Ian F. Blake

University of Waterloo

Dowden, Hutchinson & Ross, Inc.
STROUDSBURG, PENNSYLVANIA

Library of Congress Catalog Card Number: 76-11767
ISBN: 0-87933-247-6

79 78 77 1 2 3 4 5
Manufactured in the United States of America

LIBRARY OF CONGRESS CATALOGING IN PUBLICATION DATA

Walker, Bruce J.
Computer security and protection structures
Bibliography: p. 121
Includes index.
1. Computers—Access control. 2. Electronic data-processing departments—Security measures.
I. Blake, Ian F., joint author. II. Title.
QA76.9.A25W34 001.6'44 76-11767
ISBN 0-87933-247-6

Exclusive distributor: **Halsted Press**
A Division of John Wiley & Sons, Inc.
ISBN: 0-470-15155-2

COMPUTER SECURITY AND PROTECTION STRUCTURES

PREFACE

Concern for computer security began when the military became a serious user. Their initial approach—shielding the computer room to prevent electromagnetic emanations, degaussing magnetic tapes, and overwriting the contents of core and drums, together with standard military physical security—was considered sufficient at the time (Turn 72A, Turn 72B, Holl73). Any problems they had, however, were greatly magnified by the advent of multiprogramming and remotely accessible time sharing in the mid-1960s.

These were not the only factors putting the spotlight on computer security, though. Computer technology made it possible for more people to use computers, and, more importantly, for more people to use computers for more applications. What naturally happened is that companies, and the government, began to depend on the computer. With a growing dependence came a growing concern for system integrity and security. Horror stories of companies failing over computer mishaps, as well as computer crimes totaling in the millions of dollars, amplified the concern. Now, with the advent of electronic funds transfer, all areas of integrity—reliability and availability of computer facilities and assurances that information will be safeguarded—as well as security—the prime method of attaining this integrity—are being carefully investigated.

Individual privacy is the other factor motivating interest in security. The advancing technology that brought the computer to so many more users also enabled it to become an information storage and retrieval device, which meant that large data bases containing much personal information could be set up. The access-control right then became a social, moral, political, and legal issue. The result is increasing pressure for control not only of what information is stored but of who may have access to it.

This monograph contains a complete survey of the applicable literature on computer security. Only a very scant discussion is made concerning the problem of privacy. The monograph is divided into three parts. Part I, ''Threats,'' attempts to explore and classify

the scope of problems outstanding at this time. With these in mind, one can better understand not only the need for more work in the area of security but also the reasoning behind the work that is being done. Part II, "Countermeasures," is central to the material presented in this monograph. Here, all levels of security relating to computers are investigated. As a result, it is possible that not all sections will be applicable to all readers. The aim, however, is to provide a comprehensive survey. Part III presents a short survey of a few currently implemented systems. This is intended to give the reader a taste for what is available, with ideas of where to search for more information.

Within Part II, the topics range from physical installation security to operating systems design. One of the topics that will become increasingly more important is the study of cryptography. More and more data are being transmitted either via computer networks or telephone lines. Cryptography, the use of privacy transformations, is the means of attaining some sort of security against transmission-line intruders.

The advent of widespread electronic funds transfer amplifies the need for work not only in transmission security but in all other fields, including operating system security, physical security, and particularly information security.

The camera-ready copy for this monograph was generated by the Photon Econosetter, driven by the PROFF formatting program under the Honeywell GCOS time-sharing system at the University of Waterloo. The authors would like to thank Mr. Rick Beach of the University of Waterloo Computer Centre for his considerable and capable assistance in producing the copy and the staff of Dowden, Hutchinson & Ross for their patient cooperation.

Bruce J. Walker
Ian F. Blake

CONTENTS

I

THREATS

INTRODUCTION

Because the possible threats to a computing facility and the information contained therein determine the security measures that should be investigated, a survey of both internal and external threats is included. Internal threats come from within the organization and are typified by fraud, embezzlement, and accidental programming and operator errors. Although external threats include the disruption of computer services, they usually come in the form of attempted access to confidential information.

Threats can be grouped into three areas: natural disasters, accidental threats, and deliberate threats. Although natural disasters, which include not only fire, water and wind but also rioting and bombing, can be classified as either accidental or deliberate, they will be discussed separately because they have different characteristics. They tend to occur infrequently, can be very damaging, and are easily detectable. Accidental errors, on the other hand, tend to be much more frequent, much less harmful, and not necessarily detectable. Deliberate threats tend to be infrequent and can be devastating, but again are not always easily spotted. For these reasons the three classifications will be discussed separately.

NATURAL DISASTER

Because natural disasters have typically been very destructive and correspondingly expensive, most of a computing

center's security budget is geared to prevent or recover from natural disasters. Some threats, together with examples of the devastation they have caused, are given next.

Fire

Fire is a problem in any organization but takes on slightly different dimensions with respect to computers for two reasons: (1) the concentration of expensive equipment and valuable information, and (2) that water, the most common cure for fire, is at least as great a threat as the fire itself.

One of the most spectacular fire disasters took place on July 3, 1959, in the Pentagon computer center. The fire was started in a vault when a 300-watt bulb was left burning on a "fireproof" ceiling. When the vault was opened, flames shot out. The entire computer area and all tapes were destroyed (Vant71). Other examples include large-scale fires in the Army Records Center in St. Louis in July 1973 and at IBM late in the same year (Weiss74).

Water

Water damage due to fire sprinklers and firemen can be more damaging than the fire itself, since computer circuits and magnetic storage media not even near the fire may be damaged. Other sources of water damage come from tropical storms such as Agnes, floods (e.g., the one caused by hurricane Celia in 1970), activities of firemen on higher floors, leakage in the computer's water cooling system, broken pipes, sewers backing up, etc. (Weiss74).

Rioting and Bombing

Around 1969 and 1970 there was a rash of computer center disasters caused by rioting and bombing. $100,000 worth of

damage was done at the Dow Chemical's computer center in Midland, Michigan, in November 1969 by war protestors who damaged tapes, cards, and manuals. In January 1969 at Sir George Williams University, students set fire to the computer center, causing $2 million damage (VanT71).

Other acts of sabotage include 56 occurrences of a computer operator's willfully destroying computer facilities in a two-year period, and striking maintenance employees of a computer manufacturer harassing a customer's data communications network.

Miscellaneous

Other natural calamities that may occur to computing centers include explosions, earthquakes, tornadoes, aircraft crashes, war, lightning, industrial chemicals or gas, sandblasting near air conditioning intakes, etc. (Weiss74).

ACCIDENTAL THREATS

Accidental threats constitute the major problem for most computer installations. Some of the typical problems are discussed next.

Magnetism

The threat of small magnets causing havoc in tape libraries is somewhat of an overworked problem, discussed in detail by Beardsley (Beard72). There is definitely a threat to information stored on magnetic tapes, since it is magnetic fields that are used to store, retrieve, and delete information. However, the magnet must be quite strong and held quite close to the tape to have any effect. What is more of a problem is sloppy storage. Temperature and humidity extremes or winding tapes too tightly

can destroy information. Devices such as transformers, which produce alternating magnetic fields, can introduce errors in magnetic storage devices.

Loss or Destruction of Cards, Printout, Source Documents, or Magnetic Tape

Most often, lost printout is the problem, and printout can usually be recreated. However, the loss of printed copies of files that have been deleted could be very costly. Lost cards could be either input data cards or source program decks. Stories such as the one about the touring garden-club matron who took a handful of punched cards from a tray as a souvenir of her visit to the data processing center (Beard72) emphasize the need for security. Destruction of cards could be caused by water, rodents, or card readers. Magnetic tape loss could be due to mislabeling in a large computing center or sending the wrong tape away from the center.

Operator Error

Most often, operator error comes in the form of mounting an important tape as a scratch tape, but rerunning jobs, restarting jobs at the wrong place, and canceling the wrong job are also errors that could be costly.

Hardware Error

Hardware error could be caused by air conditioning failure, room temperatue and humidity deviations, brief changes in line voltages, complete power failures, or transient or permanent hardware logic errors. The result could be a head crash on a disk, where much of the information will be permanently lost, the malfunctioning of a tape drive such that it does not write the data that it should, the disabling of memory bounds registers so that one user program can overwrite another or the operating

system, and decoding failures or communication system switching errors, which can cause information to be transmitted to the wrong terminal or erroneous information to be stored on a file or processed. One hears about the computer printing out a check for $1,000,000, but not about the number of times daily jobs have to be rerun because of transient hardware failures. When the transient error stops being transient, it is possible to track it down and fix it, but in the meantime the computer is down. This loss of computer time is a real threat, and some allowance must be made for it in operations' schedules. What is sometimes more threatening than computer downtime, from a security standpoint, is hardware logic errors, which do not cause the system to malfunction but rather just compromise the hardware security. In his article (Molho70) on the hardware aspects of secure computing, Molho states that in a study done on a 360/50 a total of 99 single-failure hazards were found in the storage protection hardware and three were found in the Problem/Supervisor state logic. Any of these hazards could compromise the system security without causing a system crash. Many more logic elements could cause the storage protecton logic to go dead; but if they failed, there would eventually be a system crash.

Crosstalk

When using the telephone communication system, data signals are subject to the same threats of crosstalk as voice signals, and most people have heard other conversations on the phone from time to time. The threat of data crosstalk is not nearly as great as for voice, though, since the signals are unintelligible to those overhearing.

Software or Programming Error

Program errors are by far the most common threat. Completely testing programs or systems of programs for all

possible cases is not economical from both computer and programmer standpoints. Thus, when a situation occurs that was not tested, or possibly not even coded for, the program may act in a way that causes garbage to be written on a file or certain data to be ignored or processed incorrectly. Also, the program could abend, which may cause loss of information, if the running procedures are not set up correctly. Programs in the testing stage represent a threat to concurrently running programs in a multiprogramming environment, since by mistake they may try to read or write data from or to segments of core that are not theirs. If proprietary information is read, this could be a security breach. If garbage is written, this could cause unpredictable results for the other program.

DELIBERATE THREATS

The prevention of accidental errors is usually referred to as *protection.* The prevention of deliberate attacks on the system is referred to as *security.* Deliberate attacks are becoming more common for several reasons. First, more and more information is being concentrated at one computer site, and computer systems have become the lifeblood of many organizations. Also, psychologically, penetration of the data processing system is a more impersonal and challenging kind of attack than rifling someone's filing cabinet. It may even give the perpetrator the added satisfaction of demonstrating human superiority over a cybernetic adversary (Dawe73). This is not the whole picture, though. The fact that penetration is relatively easy has a great effect. With the advent of timesharing, some forms of attack could be considered analogous to trying to break into a safe when you have the safe in your own home without anyone knowing.

Deliberate threats have been subdivided into three areas: (1) threats that do not require the subverter to be a user of the system, such as physical threats and data communication line

threats; (2) threats that may allow the subverter to become an illegal user, in particular, threats to obtain user codes and passwords; and (3) threats that require the infiltrator to be a user, whether he is legitimate or not. Many of the threats to become illegal computer users are carried out for the purpose of taking over the system or accessing confidential files.

Deliberate Threats Not Involving Computer Users

One of the most basic threats is that of divulgence of information via waste material. Many jobs have to be rerun for one reason or another and the first output is discarded. Perhaps a new copy of a report is obtained, so the old one is thrown away. Carbon paper from multiple-copy forms can also be a threat. This waste is usually just set outside on the loading ramp for the garbage man or whoever else might be interested in the information.

Akin to this problem is the tape residue problem. Tapes that were used by one customer of a computer utility might not be needed and might subsequently be sent to another customer, who could easily read any information left on the tape. Even if the data had been erased from the tape first, the Watergate scandal reminds us that there are means of extracting the erased information.

Slightly more elementary is over-the-shoulder eavesdropping, or the scanning of someone else's card input or printed output. Important information, particularly user account codes and passwords, can be obtained this way unless safeguards are set up. Procedural safeguards to avoid nonauthorized exposure to confidential materials are often not implemented. A case in point is the "company in the highly competitive oil industry which housed its dp center in a $7 million fortress only to entrust highly proprietary printout to a commercial messenger service" (Wess71).

Theft is a threat that is, often for convenience sake, somewhat overlooked. Program listings, cards, tapes, and confidential output are left on programmers' desks overnight so that they can get back to work quickly the next day. Since the security in programming or office areas is not nearly as tight as in the computer room itself, even petty thieves could duplicate or steal information without being noticed.

Theft by company personnel is more common, however. One software thief worked on geophysical programs for an oil company. He took copies of the programs home to work on, and eventually tried to sell them to other oil companies (VanT 70A). Another group, who worked for BOAC, expropriated information about programmed systems costing $100 million and used it in consultancy work (VanT70A). In 1970, three former Encyclopedia Britannica computer operators were indicted for the theft of mailing lists valued at $3 million (Beard72). Organized crime, together with theft of a computer printout of Diner's Club customers, was used by a gang to defraud Diner's Club of at least $1 million in 1968. The printout was used to make forged cards which could be used undetected for up to 60 days (VanT70A).

To disrupt the operations of a company renting time from a computer utility, an individual could illegally authorize the release of important master file tapes. This could be a serious threat unless strict authorization was a standard practice.

Input data tampering is another nontechnical threat. The fabrication of some $2 billion worth of insurance policies in the Equity Funding scandal is perhaps the most blatant example (Weiss74). Other more subtle examples can be found. One such case was that of a young man who noticed that the personalized deposit slips for his bank had magnetically imprinted account numbers on the bottom. The ones at the bank had a dummy number. He inserted some with his number at the bank and the computer deposited the money into his account instead of flagging the deposit to be handled manually. Supposedly, he made $50,000 in one day and has not been seen since (VanT70A, Amir71, Wass69).