NCE & TECHNOLOGY:

AN ANALYSIS OF COMPUTER SECURITY SAFEGUARDS FOR DETECTING AND PREVENTING INTENTIONAL COMPUTER MISUSE

NBS Special Publication 500-25
U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards

0-25

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards[1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, the Office for Information Programs, and the Office of Experimental Technology Incentives Program.

THE INSTITUTE FOR BASIC STANDARDS provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations; and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of the Office of Measurement Services, and the following center and divisions:

Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Center for Radiation Research — Laboratory Astrophysics[2] — Cryogenics[2] — Electromagnetics[2] — Time and Frequency[2].

THE INSTITUTE FOR MATERIALS RESEARCH conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials, the Office of Air and Water Measurement, and the following divisions:

Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

THE INSTITUTE FOR APPLIED TECHNOLOGY provides technical services developing and promoting the use of available technology; cooperates with public and private organizations in developing technological standards, codes, and test methods; and provides technical advice services, and information to Government agencies and the public. The Institute consists of the following divisions and centers:

Standards Application and Analysis — Electronic Technology — Center for Consumer Product Technology: Product Systems Analysis; Product Engineering — Center for Building Technology: Structures, Materials, and Safety; Building Environment; Technical Evaluation and Application — Center for Fire Research: Fire Science; Fire Safety Engineering.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus wthin the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consist of the following divisions:

Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

THE OFFICE OF EXPERIMENTAL TECHNOLOGY INCENTIVES PROGRAM seeks to affect public policy and process to facilitate technological change in the private sector by examining and experimenting with Government policies and practices in order to identify and remove Government-related barriers and to correct inherent market imperfections that impede the innovation process.

THE OFFICE FOR INFORMATION PROGRAMS promotes optimum dissemination and accessibility of scientific information generated within NBS; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System; provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Standards — Office of International Relations.

---

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.

[2] Located at Boulder, Colorado 80302.

COMPUTER SCIENCE & TECHNOLOGY:

An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse

Brian Ruder and J.D. Madden

Stanford Research Institute
Menlo Park, California 94025

Robert P. Blanc, Editor

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, Secretary

Dr. Sidney Harman, Under Secretary

Jordan J. Baruch, Assistant Secretary for Science and Technology

U.S. NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Acting Director

Issued January 1978

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

National Bureau of Standards Special Publication 500-25
Nat. Bur. Stand. (U.S.), Spec. Publ. 500-25, 80 pages (Jan. 1978)
CODEN: XNBSAV

Library of Congress Cataloging in Publication Data

Ruder, Brian.

An analysis of computer safeguards for detecting and preventing intentional computer misuse.

(Computer science & technology) (NBS special publication; 500-25)
Supt. of Docs. no.: C13.10:500-25

1. Computer crimes. 2. Computers—Access control. 3. Electronic data processing departments—Security measures. I. Madden, J. D., joint author. II. Title. III. Series. IV. Series: United States. National Bureau of Standards. Special publication ; 500-25.
QCI00.U57 no. 500-25 [HV6773] 602'.Is [364.1'62] 77-25368

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1978)

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402. Price $2.40—Stock No. 003-003-01871-6

PREFACE

The work reported here was performed at Stanford Research Institute (SRI) for the National Bureau of Standards (NBS). The objectives of the study are to:

(1) Develop a working definition of intentional computer misuse and a taxonomy to characterize the different types of intentional computer misuse.
(2) Develop a ranked list of specific detection mechanisms.
(3) Develop a ranked list of specific prevention mechanisms.

The detection and prevention mechanisms were to be developed as a result of analysis of computer misuse case files, most of which are maintained by Mr. Donn B. Parker of SRI.

Robert P. Blanc, Editor
Staff Assistant for Computer
Utilization Programs
Institute for Computer Sciences
and Technology

TABLE OF CONTENTS

ILLUSTRATIONS

TABLES

AN ANALYSIS OF COMPUTER SECURITY SAFEGUARDS FOR DETECTING AND PREVENTING INTENTIONAL COMPUTER MISUSE

Brian Ruder
J. D. Madden
Stanford Research Institute
Menlo Park, California 94025

ABSTRACT

Stanford Research Institute (SRI) has an extensive file of actual computer misuse cases. The National Bureau of Standards asked SRI to use these cases as a foundation to develop ranked lists of computer safeguards that would have prevented or detected the recorded intentional misuses.

This report provides a working definition of intentional computer misuse, a construction of a vulnerability taxonomy of intentional computer misuse, a list of 88 computer safeguards, and a model for classifying the safeguards. In addition, there are lists ranking prevention and detection safeguards, with an explanation of the method of approach used to arrive at the lists.

The report should provide the computer security specialist with sufficient information to start or enhance a computer safeguard program.

KEY WORDS

Computer security; computer misuse; computer safeguards; computer security model; computer crime; computer fraud; privacy.

I. INTRODUCTION

A primary objective of this report is to identify computer safeguards that would have been useful in detecting and preventing actual cases of computer misuse. Section VI contains safeguard rankings based on cases of past intentional computer misuse. These cases span the spectrum of computer misuse, but the number of cases that fall into each vulnerability category probably do not reflect any one specific computer environment. Generally speaking, the highest ranking safeguards should be best in most environments, but the ranking process is somewhat subjective due to the nature of the cases and degree of detail specified in the safeguard description. Therefore, the rankings should not be considered absolute. Computer specialists should consider all tools as they develop their computer protection plan. A set of tools and a description of their purpose and application is provided in Appendix B.

This report contains the results of six work efforts, each of which is briefly described below.

The first effort involved developing a taxonomy of computer vulnerability to intentional computer misuse. The computer vulnerability taxonomy forms the foundation for the definition of intentional computer misuse as well as the foundation for categorizing past cases of computer misuse. Section II of this report contains this taxonomy.

The second effort was to develop a working definition of intentional computer misuse. The persons known to be studying the area of computer misuse throughout the country were contacted to determine their current definitions relating to computer abuse or computer misuse. The resulting definition of intentional computer misuse and a discussion of how the definition was arrived at are addressed in Section III of this report.

The third effort was to review the case file of computer misuses and distribute cases into appropriate vulnerability categories. Each case was placed in only one vulnerability category even though three or four misuses may have been identified in the case writeup. Each case was placed in the category corresponding to the first misuse identified in the case writeup.

The fourth effort was to review case files to identify the prevention and detection safeguard mechanisms in each case that would have mitigated the misuses in that case. The safeguards from a previous NSF study[1] as well as those gathered from other relevant source material were used as a base and were supplemented by the authors' experiences and ideas.

---

[1] "Computer System Integrity Research Program," National Science Foundation Grant DCR74-23774.