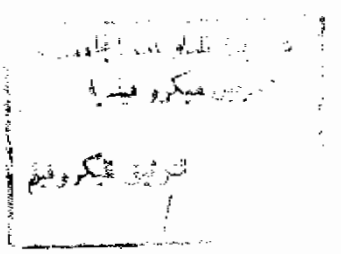
Ain Shams University
Faculty of Science

A thesis submitted to the
Department of Mathematics



On Computer Security

In partial fulfellment of requirement for
Master Degree of Computer Science

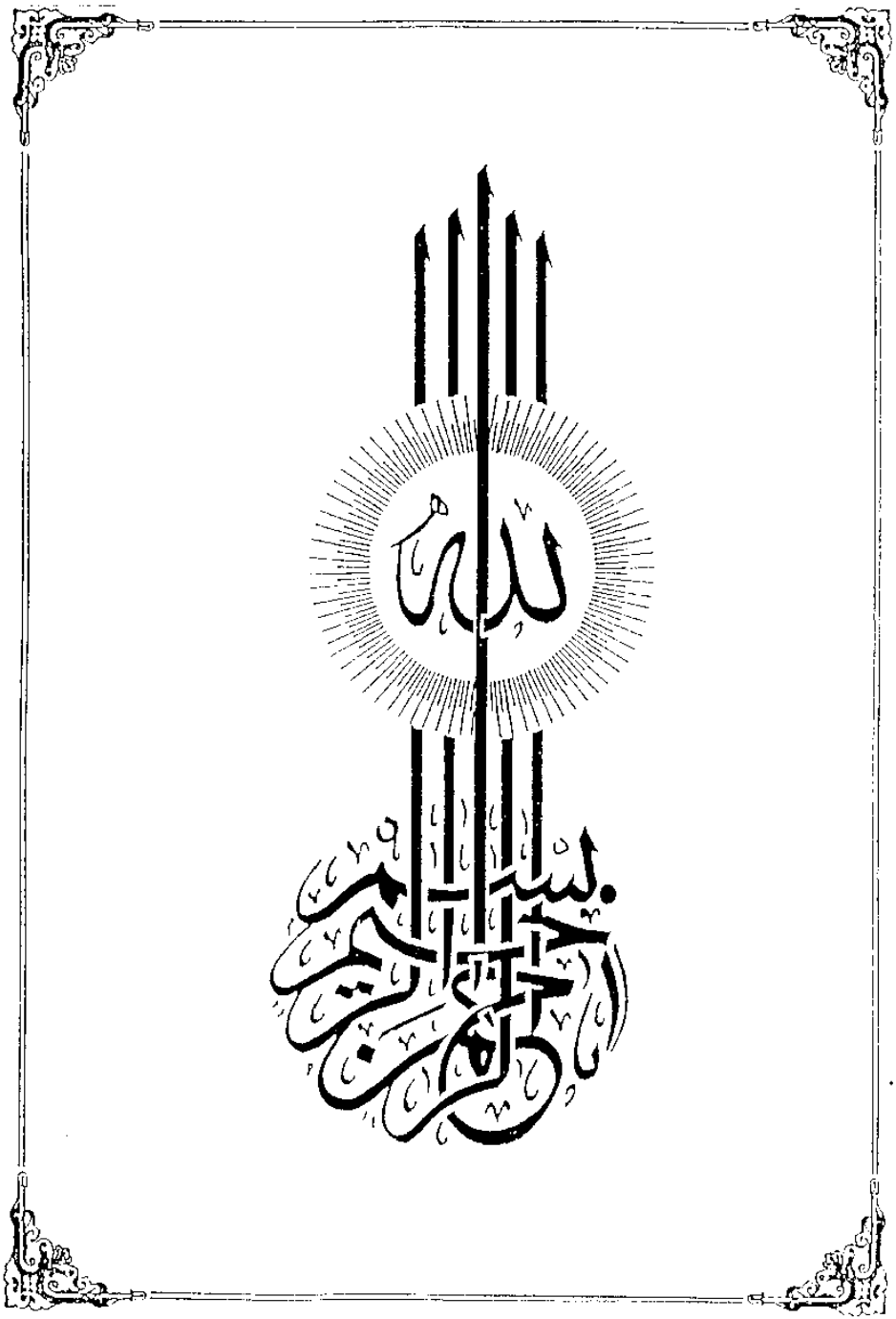
By

Abd El Nasser Hassan Ahmed Odah

Supervised by

Dr. Fayed Fayek Mohamed Ghaleb
Dr. Mohamed Sadek Esmaiel

1993



Acknowledgment

The author wishes to express his gratitude to Dr. Mahmod Khairat Ahmed Khairat for his constructive help and advise.

The author owes a debt of gratitude to his research advisors both Dr. Fayed Fayek, and Dr. Mohamed Sadek, for their talented quidance, energetic support, qualified Advice, and patient reviews.

The list of thanks should be extended to include all the faculty members.

This acknowledgment is never complete without a word of appreciation to my parent and my family for providing all the facilities and assistance to complete my research successfully.

Preface

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1990s. As we come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Computer security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure and modification.

The goal of this thesis is to study the computer security based on three main component parts - privacy, integrity and availability. Privacy implies the property of preventing the disclosure of information to unauthorized parties, either as a result of accident or of deliberate attack. Integrity implies the prevention of unauthorized alteration of information, again either as a result of accident or of deliberate attack. Availability implies ensuring that a system is available to authorized users at all times intended by the system owner; denial of service as a result of deliberate attack is one of the conditions to be protected against here.

This thesis consists of an introduction, six chapters, and one appendix. Introduction (chapter 0 "The Need For Security") starts by a historical background then presents the physical security and technological countermeasures.

Here is a brief summary of other chapters:

- **Chapter 1,** ***Access Controls***, describes the basic principles of mechanisms that control access by subjects(e.g., users or programs) to objects (e.g., files and records).

- **Chapter 2,** ***How to Design an Effective Auditing Subsystem,*** summarizes the auditing subsystem requirements for a CMW, and an effective method for building these subsystems.

- **Chapter 3,** ***Understanding DES "The Data Encryption Standard"***, describes both the classical and modern encryption algorithms, including a full detail understanding the DES and public-key algorithms.

- **Chapter 4,** ***Viruses and Trojan Horses,*** gives the definitions of virus , types of viruses, and the prevention/detection of viruses. This chapter includes a comparison of virus protection products.

- **Chapter 5,** ***A Model of Access Control Policy,*** introduces a general model for access control policy for sensitive information.

- **Chapter 6,** A source code program, ***"Access Control on IBM/PC."***

- **References**

- **Appendix A,** A glossary of security terms.

Table of Contents Page

Acknowledgement 1
Preface 2
Table of Contents 4

Chapter 0: Introduction 8-16

0.1: Historical Background 8
0.2: Physical Security 11
0.3: Technological Countermeasures 13
0.4: Conclusion 16

Chapter 1: Access Control 17-54

1.1: Access-Matrix Model 17
1.1.1: The Protection State 17
1.1.2: State Transitions 19
1.1.3: A Key-Lock Pair Mechanism 19
1.1.4: The Key-Lock Pair Mechanism Based Upon EULER's Theorem 23
1.2: Access Control Mechanisms 26
1.2.1: Security and Precision 26
1.2.2: Reliability and Sharing 27
1.3: Access Hierarchies 32
1.3.1: Privileged Modes 32
1.3.2: Nested Program Units 34
1.4: Authorization Lists 34
1.4.1: Owned Objects 35
1.4.2: revocation 37
1.5: Capabilities 40
1.6: Verifiably Secure Systems 42
1.7: Security Control and Procedures 45
1.7.1: User Identification 45
1.7.2: User Authentication 45
1.7.3: Login Control 46
1.7.4: Password Management 46
1.7.5: Authorization 47
1.7.6: Journaling/Logging 47
1.7.7: Auditing 47
1.7.8: Scavenging Countermeasures 47

Page

1.8: Trusted Computer System Evaluation Criteria (TCSEC) 49
1.8.1: TCSEC Divisions and Classes 49
1.8.2: Trusted Product Evaluation 53

Chapter 2: How to Design an Effective Auditing Subsystem 55-72

2.1: Introduction 55
2.2: Audit Data 56
2.2.1: Data Collection 58
2.2.2: Data Storage 59
2.3: Auditing Subsystem Design 59
2.3.1: Overview 59
2.3.2: User Interface 60
2.3.3: Application Level 61
2.3.4: User/Operating System Interface Level 64
2.3.5: Operating System Interface Level 65
2.3.6: The audit_write() Kernel Subroutine 65
2.3.7: Data Compression 66
2.4: Audit Reduction Overview 70
2.5: Conclusions 72

Chapter 3: Understanding DES The Data Encryption Standard 73-120

3.1: Ground Rules and Terminology 73
3.1.1: Terminology 73
3.1.2: Avoided Code Terminology 75
3.1.3: Codes Versus Ciphers 75
3.2: The Data Encryption Standard 78
3.2.1: Origins 78
3.2.2: Native DES: ECB Mode 79
3.2.3: Bit Sensitivity 80
3.2.4: The Basic Building Blocks of the DES 81
3.2.5: Piecing the DES Together 86
3.2.6: The Final Assembly 88

Page

3.2.7: The Ramifications of the Round 91
3.2.8: The FIPS Ladder Diagram 94
3.3: The Key Scheduler 97
3.4: Other Modes of DES 100
3.4.1: Return to ECB Mode 100
3.4.2: CBC Mode 101
3.4.3: The Feedback Modes 104
3.5: Modes 110
3.6: DES Security A Final Word 110
3.7: Public-Key Cryptography 111
3.7.1: Knapsack Ciphers 113
3.7.2: Obvious Advantages of Public Keys 116

Chapter 4: Viruses and Trojan Horses 121-139

4.1: Definition 121
4.2: History 123
4.3: Types of Malicious Programs 125
4.4: Types of Viruses 128
4.5: Significant Viruses and Related Incidents 130
4.6: Prevention/Detection 132
4.7: Virus Protection Products 134
Comparison Column Entry Descriptions

Chapter 5: **A Model of Access Control Policy** 140-162

5.1: Introduction 140
5.2: Related Work 141
5.3: Basic Principles 142
5.4: Access Control Policy Model 143
5.5: Application of Model to IRS Requirements 157
5.6: Conclusions 162

Chapter 6: A source code program, **"Access Control on IBM/PC."** 163-197

References 198-200

Appendix A: **A glossary of security terms.** 201-207

Figure **Page**

1-1 Access matrix 18
1-2 Protection system 20
1-3 Security and precision 26
1-4 Suspicion 27
1-5 Torjan Horse 28
1-6 The confinement problem 30
1-7 Mutual suspicion 30
1-8 The protection rings 33
1-9 Hierarchical rings structure 33
1-10 Block structured program 34
1-11 Authorization list for file 35
1-12 UNIX file directory tree 36
1-13 Transfer of rights for relation X 39
1-14 Transfer of rights for relation Y 39
1-15 Capability list 41
1-16 ULCA secure UNIX architecture 42
1-17 KSOS-11 architecture 44

2-1 Events to be audited 57
2-2 The five system calls 61

3-1 A ciphering algorithm 74
3-2 A sample code book 76
3-3 A DES encryption and decryption 79
3-4 A P-box 81
3-5 The XOR cryption algorithm 83
3-6 An S(Substitution)-box 85
3-7 Piecing the DES together 86
3-8 A DES round 89
3-9 A DES round , the compact representation 91
3-10 The first DES recirculation 93
3-11 The FIPS lader diagram 95
3-12 The key scheduler 98
3-13 Cipher Block Chaining (CBC) mode 102
3-14 A K-bit Output Feedback (OFB) mode 106
3-15 A K-bit Cipher Feedback (CFB) mode 109
3-16 One-way function 112
3-17 Algorithm snap (C,A) "Sample Knapsack solution" 114

4-1 Batch file virus 123
4-2 Virus protection products, a comparison column 136

Chapter

0

Introduction

"The Need for Security"

Chapter 0
Introduction
The Need for Security

0.1 Historical Background

The 1940s and '50s

Early computers were operated by the same individuals who programmed and repaired them. These pioneers were not so concerned about the security of information as they were with simply getting these huge vacuum tube-equipped machines to execute the desired instructions. Security revolved primarily around limiting physical access to prevent outsiders from tampering with the hardware, and maintaining environmental cooling systems essentially to these heat-generating electromechanical monsters.

The development of the transistor in the late 1950s made smaller, faster, and more versatile computers possible. Both the public and private sectors began to realize the importance of computers.

The 1960s - Computer Security

As the transistor revolutionized the computer industry, the capabilities of computers appeared almost limitless. Large mainframe computer environments were considered showcases, proudly displayed to employees and customers primarily to impress everyone with the technological prowess of the organization.

In the late 1960s, organizations that increasingly relied on their computers for day-to-day business realized that showcasing this asset was not in their best interest. Threats of violence against government, corporate, and educational computer operations centers caused these organizations to secure the computer operations facility, an attitude now referred to as the "fortress mentality."

The term *computer security* implied protection of the computer itself. Physical security was the primary concern. Security measures included fire protection and site access control. Since batch oriented application required very limited interface by users, computer operators were the only human interface other than programmers or vendor personnel. *Security of the information was not perceived as the most critical issue.*

The introduction of silicon-based technology in the latter half of the decade made possible the concentration of many transistors on one integrated circuit. This dramatic improvement in computer technology provided for smaller,more reliable,and less expensive computers.

This advance made computers available to all those who had previously been unable to justify their use.The result was another sharp increase in the number of computer applications.

The 1970s - Data Security

Increases in productivity and benefits of instant access to large amounts of data shifted the focus of security from physical control of the mainframe computer to control of data. The shift to *data security* was accompanied by implementation of simple password control capabilities coupled with enhanced physical security measures, such as Halon fire suppression system,off-site storage of data and software, and disaster recovery planning.

Continued improvement of the technology provided faster, less expensive computers communications hardware. User demand for interactive systems mushroomed. Online realtime applications, designed to permit many users access to the same data, began batch systems and spurred user demand for faster development of online interactive systems.

To circumvent the lengthy lead times required in large centralized date processing environments,users turned to minicomputers and the newly introduced personal computers. End-user computing requirements began to drive the data processing industry.

The 1980s / 1990s Information security

The stage is now set for *information security*. Mainframe computers, minicomputers, and microcomputers are essential equipment in businesses, schools, and government offices throughout the world. Midrange systems and microcomputers, with expanding internal storage capabilities, store huge quantities of information. Low-cost personal computers are often used to access mainframe information.

Data stored on mainframe computers now can be accessed through telephone lines by many users.

The concentration of complete processes,and the reliance upon timely and accurate information,has mandated that the focus of security shift from data to information.

The future of computers is already becoming quite clear. Continued reliance on mainframe and distributed computing systems together with expansion of end-user computing systems and networks , demonstrate that the sky is the limit for use of computer technology. Decisions made and actions taken as a result of computerized output, however, are only as good as the information input.

Information integrity, confidentiality, and availability, must be maintained in order to ensure the quality and accuracy of the end result. Appropriate information security measures can reduce organizational exposures and vulnerabilities.

Information security is really the protection of information integrity, availability, and confidentiality.

The Year 2000 and Beyond

What's next? Some say that the buzzword of future is "knowledge security."

Artificial intelligence, miniaturization of hardware and firmware components, light speed-type data communications rates, interactions between systems and networks, as well as other developments, will serve as building blocks for the gathering, concentration,and application of human knowledge.

0.2 Physical Security

Most experts agree that physical security expenditures should concentrate on the following:

1- Physical access control measures for both outsiders and unauthorized insiders;
2- Preventing, detecting, and limiting damage due to water leakage; and
3- Protection against loss of operational capabilities due to electrical power failure or fluctuations.

It is important to understand, that meaningful information security can only be achieved after appropriate physical security measures have been implemented.