



Cairo University
Institute of Statistical Studies and Research
Department of Computer and Information Sciences

A SECURITY POLICY BASED ON DATA INTEGRITY VERIFICATION

A thesis submitted to the Department of Computer and Information Sciences,
Institute of Statistical Studies and Research, Cairo University, in partial
fulfillment of the requirements for the degree of Master of Science in the
Computer and Information Sciences.

By

Omar Hussein Sayed Mohamed

Supervised By

Prof. Dr. Eng. Osman Hegazy Mohamed

Department of Information Systems

Faculty of Computers and Information - Cairo University

Prof. Dr. Amany Mousa Mohamed

Department of Applied Statistics

Institute of Statistical Studies and Research - Cairo University

Dr. Eng. Fatma A. El-Licy

Department of Computer and Information Sciences

Institute of Statistical Studies and Research - Cairo University

Cairo, 2009

STATEMENT

I certify that this work has not been accepted in substance for any academic degree and is not being concurrently submitted in candidature for any other degree.

Any portions of this thesis for which I am indebted to other sources are mentioned and explicit references are given.

Student: Omar Hussein Sayed Mohamed

APPROVAL SHEET

A SECURITY POLICY BASED ON DATA INTEGRITY VERIFICATION

MASTER DEGREE THESIS

Submitted By
Omar Hussein Sayed Mohamed

A thesis submitted to the Department of Computer and Information Sciences, Institute of Statistical Studies and Research, Cairo University, in partial fulfillment of the requirements for the degree of Master of Science in the Computer and Information Sciences. This thesis has been approved by:

Name	Signature
Prof. Dr. Eng. Osman Hegazy Mohamed	
Prof. Dr. Amany Mousa Mohamed	
Prof. Dr. Eng. Tarek Abdel Megeed Abdel Aziz	
Prof. Dr. Eng. Bahaa Eldin Mohamed Hasan	

Date: / / 2009

"

"

Dedication

Words can never express my deep gratitude to my dear Mother. She continuously invokes ALLAH to provide me with success and guidance. I exclusively dedicate this thesis, and any success I achieve to my dear Mother.

Acknowledgement

All gratitude is due to ALLAH who made this success possible. I am deeply grateful to my dear Mother, Father, and Brother for their continuous care, encouragement, and endless support.

I was proud to work under the supervision of Prof. Dr. Eng. Osman Hegazy; the main supervisor. I wish to express my sincere thanks for his guidance, valuable advices, and extensive support.

Deepest thanks to Prof. Dr. Amany Mousa for her supervision, and support.

I wish to express my special thanks and appreciation to Dr. Eng. Fatma A. El-Licy for her supervision, fruitful technical directions, and constructive advice.

Great thanks to Dr. Eng. Hesham Hefny; the head of computer and information sciences department, and the staff members, for their assistance and kind help.

Abstract

Data is valuable, only, when it is correct and accurate. In this thesis, focus is driven towards safeguarding stored data integrity from new malicious software (Malware) attacks, and unauthorized modification attacks committed by insiders. Computer crime and security surveys, however, revealed that, despite of the wide use of anti-virus software and Access Control Lists (ACLs) security mechanisms to counter those two types of threats, they are insufficient and ineffective. Therefore, this work is motivated to minimize the negative effects of such attacks.

This thesis is devoted to analyze, design, and implement a security mechanism to verify data integrity. This mechanism forms an additional data security layer underneath that of ACLs to detect and prevent unauthorized modification to critical configuration and data files. It integrates Biba strict integrity mandatory access control security policy with the *verification by comparison* data integrity assurance method. It aims at detecting the existence of new Malware, limiting its damaging effects, and preventing usage of ill-gotten access rights.

The mechanism's security functional requirements were mapped into those mentioned in standard number 15408 produced by the International Organization for Standardization (ISO). This standard addresses protection of information from unauthorized modification and disclosure. It provides a common set of requirements for the security functions of information technology products and systems. Such mapping insured -to a high extent- that the mechanism fulfilled standardized functionality.

Key Words: Data Security, Security Policy, Multilevel Security, Data Integrity Verification, Access Control, ACL, DAC, MAC, ISO 15408.

CONTENTS

ABSTRACT	vii
CONTENTS	viii
LIST OF ABBREVIATIONS	x
LIST OF SYMBOLS	xii
LIST OF FIGURES	xiii
LIST OF TABLES	xv
CHAPTER 1: INTRODUCTION	1
1.1. BACKGROUND	2
1.2. THESIS TOPIC, SCOPE, AND CONTRIBUTION	3
1.3. MOTIVATION AND PROBLEM SPECIFICATION	4
1.4. RESEARCH QUESTIONS	7
1.5. THESIS OBJECTIVES	7
1.6. THESIS ORGANIZATION	7
CHAPTER 2: DATA SECURITY FUNDAMENTALS	9
2.1. DATA SECURITY ASPECTS	10
2.1.1. Data Security Facets	11
2.1.2. Data Integrity Higher Precedence Over Confidentiality and Availability ..	12
2.1.3. Data Security Concepts	12
2.2. DATA SECURITY PLAN PHASES	14
2.2.1. Inspection Phase	14
2.2.2. Protection Phase	15
2.2.3. Detection Phase	19
2.2.4. Reaction Phase	20
2.2.5. Reflection Phase	20
CHAPTER 3: SECURING DATA INTEGRITY	21
3.1. THREATS	22
3.1.1. New Malware's Attacks	23
3.1.2. Unauthorized Access Attacks Committed by Insiders	26
3.2. SAFEGUARDS	27
3.2.1. Anti-Virus Software	27
3.2.2. Access Control Security Policies, Models, and Mechanisms	27
3.3. DATA INTEGRITY ASSURANCE METHODS	34
3.3.1. Verification	34
3.3.2. Limited Use	35
CHAPTER 4: VULNERABILITIES IDENTIFICATION AND BIBA SECURITY MODEL	36
4.1. VULNERABILITIES IDENTIFICATION	37
4.1.1. Anti-virus Software Gap	37
4.1.2. ACLs Operation and Misuse	37
4.2. BIBA SECURITY MODEL	40
4.2.1. Security Policies Supported by Biba Model	41
4.2.2. Chosen Security Policy	44
CHAPTER 5: A PROPOSED SECURITY MECHANISM TO VERIFY DATA INTEGRITY	46
5.1. MECHANISM OBJECTIVES	47
5.1.1. Detect the Existence of New Malware	47
5.1.2. Limit New Malware's Damaging Effects	47
5.1.3. Prevent Using ILL-Gotten Access Rights	48
5.2. DIG AND ISO 15408 INTERNATIONAL STANDARD	50

5.3. DIG's PROCESS MODELING	54
5.3.1. Functional Decomposition Diagrams	54
5.3.2. Data Flow Diagrams	62
CHAPTER 6: MECHANISM DEMONSTRATION	72
CHAPTER 7: CONCLUSIONS AND FUTURE WORK	92
7.1. SUMMARY OF THESIS CONCLUSIONS AND CONTRIBUTION	93
7.1.1. Conclusions	93
7.1.2. Contribution	94
7.2. DIRECTION FOR FUTURE WORK	95
REFERENCES	96

LIST OF ABBREVIATIONS

A	Audit log
ACL	Access Control List
ACSP	Access Control Security Policy
BLP	Bell-Lapadula
C	Categories
CERT	Computer Emergency Response Team
CSI	Computer Security Institute
D	Data store
DAC	Discretionary Access Control
DIG	Data Integrity Guard
DOS	Denial Of Service
DSF	Data integrity guard Security Functions
FBI	Federal Bureau of Investigations
FDP	Functional user Data Protection
FDP_ACC	Access Control policy
FDP_ACF	Access Control Functions
FDP_ITC	Import from outside Target of evaluation security functions Control
FDP_SDI	Stored Data Integrity
FIA	Functional Identification and Authentication
FIA_ATD	user Attribute Definition
FMT	Functional security Management
FMT_MSA	Management of Security Attributes
FPT	Functional Protection of the Target of evaluation security functions
FPT_RVM	Reference Mediation
I/O	Input/Output
ICSA	International Computer Security Association
IDS	Intrusion Detection Software
IL	Integrity Labels
il	an integrity label
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
L	security Levels
l	a security level
LAN	Local Area Network
MAC	Mandatory Access Control
Malware	Malicious software

MLS	Multilevel Security
O	Objects
o	an object
p	power set
RA	Risk Analysis
S	Subjects
s	a subject
SF	Security Function
SFP	Security Function Policy
SL	Security Labels
sl	a security label
TOE	Target Of Evaluation
TSC	Target of evaluation security functions Scope of Control
TSF	Target of evaluation Security Functions
TSP	Target of evaluation Security Policy
V	Integrity Levels
v	an integrity level

LIST OF SYMBOLS

$\%$	Percent
Σ	Summation
$\$$	Dollars
$\forall$	For all
$\in$	Belongs to
$\wedge$	And
$\Rightarrow$	Then
$\Leftrightarrow$	If and only if
$\geq$	Dominates
$>$	Greater than
$<$	Less than
$=$	Equals
$\subset$	Subset
$ $	Cardinality measure
$*$	Cartesian product
Φ	Empty set

LIST OF FIGURES

Figure 1.1:	Thesis's scope	3
Figure 1.2:	Dollar amount of losses by type of attack during 2005 [Csi and Fbi, 2005]	5
Figure 1.3:	Dollar amount of losses by type of attack during 2006 [Csi and Fbi, 2006]	5
Figure 1.4:	Used security technologies by survey respondents during 2005 [Csi and Fbi, 2005]	6
Figure 1.5:	Used security technologies by survey respondents during 2006 [Csi and Fbi, 2006]	6
Figure 2.1:	Relationships between main data security terms [Iso_1, 2005]	11
Figure 2.2:	Data security facets	11
Figure 2.3:	Relationships between main data security concepts	13
Figure 2.4:	Data security design levels and security enforcement direction	15
Figure 2.5:	Security policy importance as stated by year 2006 percentage of survey respondents [Csi and Fbi, 2006]	17
Figure 2.6:	System's states partitioned by the access control security policy	17
Figure 2.7:	The security policy violation effect on system's states	18
Figure 2.8:	Access control security mechanism's complete mediation	18
Figure 3.1:	Number of reported security incidents from 1999 to 2003 [Cert, 2003]	23
Figure 3.2:	Virus program flowchart	25
Figure 3.3:	Basis for access requests evaluation in MLS	28
Figure 3.4:	An Access Control Matrix	29
Figure 3.5:	ACLs example	30
Figure 3.6:	Capabilities Lists example	31
Figure 3.7:	Data flow direction in Bell-LaPadula model	33
Figure 3.8:	Allowed actions in BLP model	33
Figure 4.1:	Anti-virus software gap	38
Figure 4.2:	Defenseless ACLs in the face of new Malware's attacks	38
Figure 4.3:	Defenseless ACLs in the face of illegal forwarding of permissions	39
Figure 4.4:	Lax enforcement of the organization's security policy	40
Figure 4.5:	Integrity star property (No-Write-Up)	41
Figure 4.6:	Simple integrity property (No-Read-Down)	42
Figure 4.7:	Data flow direction in Biba strict integrity access control security policy	42
Figure 4.8:	Pathway to the proposed security mechanism	45
Figure 5.1:	DIG's ability to detect the existence of new Malware and limit its damaging effects	48
Figure 5.2:	DIG's ability to prevent using ill-gotten access rights	49
Figure 5.3:	DIG's initial functional decomposition diagram	54
Figure 5.4:	Functional decomposition diagram of "Detect Existence of New Malware" function	55
Figure 5.5:	Functional decomposition diagram of "Generate Integrity Labels" sub-function	55
Figure 5.6:	Functional decomposition diagram of "Import Files Golden States" sub-function	56
Figure 5.7:	Functional decomposition diagram of "Verify Files Data Integrity" sub-function	56
Figure 5.8:	Full functional decomposition diagram of "Detect Existence of New Malware" function	57
Figure 5.9:	Functional decomposition diagram of "Prevent Insiders Unauthorized Modification" function	58
Figure 5.10:	Functional decomposition diagram of "Assign Integrity Labels to Users" sub-function	58

Figure 5.11:	Functional decomposition diagram of "Enforce Biba Security Policy Rules" sub-function	59
Figure 5.12:	Full functional decomposition diagram of "Prevent Insiders Unauthorized Modification" function	60
Figure 5.13:	DIG's full functional decomposition diagram	61
Figure 5.14:	DIG's context diagram	62
Figure 5.15:	Data flow diagram of DIG's two main process	63
Figure 5.16:	Data flow diagram of "Detect Existence of New Malware" process	64
Figure 5.17:	Data flow diagram of "Generate Integrity Labels" sub-process	65
Figure 5.18:	Data flow diagram of "Import Files Golden States" sub-process	66
Figure 5.19:	Data flow diagram of "Verify Files Data Integrity" sub-process	67
Figure 5.20:	Data flow diagram of "Prevent Insiders Unauthorized Modification" process ...	68
Figure 5.21:	Data flow diagram of "Assign Integrity Labels to Users" sub-process	69
Figure 5.22:	Data flow diagram of "Enforce Biba Security Policy Rules" sub-process	70
Figure 5.23:	DIG's full data flow diagram	71
Figure 6.1:	DIG's main screen	73
Figure 6.2:	Automatic integrity labels generation	74
Figure 6.3:	Screen used to capture critical file's Golden state	75
Figure 6.4:	Locate and choose a critical file to monitor	75
Figure 6.5:	Captured critical file's Golden state	76
Figure 6.6:	Save critical file's Golden state	77
Figure 6.7:	Successful saving of critical file's Golden state	77
Figure 6.8:	Locate and choose the Golden state file	78
Figure 6.9:	Retrieve critical file's Golden state	78
Figure 6.10:	Assign an integrity label to a user	79
Figure 6.11:	Successful integrity label assignment to the first user	80
Figure 6.12:	Successful integrity label assignment to the second user	80
Figure 6.13:	Successful integrity label assignment to the third user	81
Figure 6.14:	Data integrity verification by comparison flow chart	82
Figure 6.15:	Locate and choose a critical file to verify its data integrity	83
Figure 6.16:	Capture and display critical file's current state	83
Figure 6.17:	Verification result for critical file's creation date and time security attribute	84
Figure 6.18:	Verification result for critical file's last modification date and time security attribute	85
Figure 6.19:	Verification result for critical file's last read access date and time security attribute	85
Figure 6.20:	Verification result for critical file's size security attribute	86
Figure 6.21:	Verification result for critical file's integrity label security attribute	86
Figure 6.22:	File's accumulated data integrity verification result	87
Figure 6.23:	Read access allowed (file's integrity label is the same as user's integrity label).....	89
Figure 6.24:	Write access allowed (user's integrity label dominates file's integrity label)	89
Figure 6.25:	Read access allowed (file's integrity label dominates user's integrity label).....	90
Figure 6.26:	Write access denied (user's integrity label does not dominate file's integrity label)	90
Figure 6.27:	Read access denied (dominance relationship does not exist)	91
Figure 6.28:	Write access denied (dominance relationship does not exist)	91

LIST OF TABLES

Table 1.1:	Losses incurred by types of attacks under study and their contribution in the annual total amount of losses [Csi and Fbi, 2005], [Csi and Fbi, 2006]	4
Table 1.2:	Used security technologies under study by percentage of respondents [Csi and Fbi, 2005], [Csi and Fbi, 2006]	4
Table 3.1:	Types of threats according to their source	22
Table 3.2:	External vs. internal threats	22
Table 3.3:	Comparison between Viruses, Worms and Trojan Horses	26
Table 3.4:	Authorization Table example	29
Table 3.5:	MAC vs. DAC	34
Table 4.1:	Problems found in Non-Strict Integrity policies	44
Table 5.1:	Required access rights to be enforced	48
Table 5.2:	Reasons for ensuring enforcement of required access rights	49
Table 5.3:	DIG's complete access control	50
Table 5.4:	DIG's security attribute based access control (1)	51
Table 5.5:	DIG's security attribute based access control (2)	51
Table 5.6:	DIG's import of user data with security attributes	51
Table 5.7:	DIG's stored data integrity monitoring	52
Table 5.8:	DIG's stored data integrity monitoring and action	52
Table 5.9:	DIG's user attribute definition	52
Table 5.10:	DIG's management of security attributes	53
Table 5.11:	DIG's Non-bypassability of the TSP	53
Table 6.1:	Mandatory access rights required to be enforced	88
Table 6.2:	Assigned integrity labels	88