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

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

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

بسم الله الرحمن الرحيم

"يرفع الله الذين آمنوا منكم والذين أوتوا العلم درجات والله بما تعملون خبير"

صدق الله العظيم

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

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
$\sum$	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

LIST OF TABLES