A(ST'S)
.S5
YAN

Detecting Suspicious Access Patterns in Secure Physical Environment

by

Yan Pengfan

Master of Science in Software Engineering

2009



Faculty of Science and Technology
University of Macau

TABLES OF CONTENTS

TABLES OF CONTENTS vi
LIST OF TABLES viii
LIST OF FIGURES ix
APPENDIX x
1. INTRODUCTION 11
1.1. Background 11
1.2. Motivation 13
1.3. Research Problem 15
1.3.1. Audit source 15
1.3.2. Detection approach 16
1.4. Outline of solution approach 17
1.4.1. Simulated access event generator 17
1.4.2. Rule-based detection 18
1.4.3. Knowledge-based detection 18
1.5. Methodology 19
1.6. The Challenge 19
1.7. Outline of thesis 20
2. RELATED WORK 21
2.1. Evolution of Intrusion Detection System 21
2.2. Prototypes of IDS 22
2.3. Technical Models of IDS 24
2.4. Data mining related 25
3. PATTERN DETECTION 28
3.1. Physical Environment Definition 28
3.1.1. Secure Physical Environment 28
3.1.2. Access Events in Tracking Path 32
3.1.3. Parameter Definition 34
3.2. Suspicious Patterns Detection 35
3.2.1. Semantics of suspicious patterns 35
3.2.2. Concrete detection algorithms 37
3.2.2.1. Detection of Temporal Pattern 38
3.2.2.2. Detection of Repetitive Pattern 38
3.2.2.3. Detection of Displacement Pattern 40
3.2.2.4. Detection of Out-of-Sequence Pattern 40
4. SIMULATED ACCESS EVENT GENERATOR 42
4.1. System Hierarchy and Modules 42
4.1.1. System Hierarchy 44
4.1.1.1. Client Layer 44
4.1.1.2. Application Servers Layer 45
4.1.1.3. Data Layer 45
4.1.2. System Modules 46

4.1.2.1. Physical Environment Module 46
4.1.2.2. Data Simulation Module 46
4.1.2.3. Real-time Tracing Module 47
4.1.2.4. Data Mining Module 47
4.1.2.5. Pattern Detection Module 47
4.2. Data Simulator 48
4.2.1. Main Entity-Relation Diagrams 48
4.2.2. VOP and VRP Algorithm for path finding 49
4.2.3. User Portion and Occurrence Distribution 57
4.3. Simulated Access Events 58
5. EXPERIMENT 60
5.1. Access Event Generator 60
5.2. Performance for Suspicious Pattern Detector 62
6. CONCLUSION 64
6.1. Summary 64
6.2. Contributions 64
6.3. Future directions 65
BIBLIOGRAPHY 66