Document téléchargé depuis www.pnst.cerist.dz CERIST

Imperial College of Science, Technology and Medicine
University of London
Department of Computing

Domain-Based Security for Distributed Object Systems

Nikolaos Yialelis

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in the Faculty of Engineering of the University of London, and for the Diploma of Imperial College of Science, Technology and Medicine.

August 1996

Corrected October 1996

Document téléchargé depuis www.pnst.cerist.dz CERIST

Abstract

Advances in telecommunications technology have resulted in the proliferation of large distributed systems in commercial environments. Distributed systems, however, are vulnerable to unauthorised access to resources and compromise of information, either in terms of integrity or confidentiality. Furthermore, a distributed system may contain a large number of objects that are mutually suspicious making it hard to specify security policy. In addition, such a system may cross organisational boundaries necessitating decentralised security management.

This thesis proposes a security architecture for distributed object systems that supports access control services based on the concept of a *domain*. Domains can be used to group objects in a hierarchical structure, to apply a common security policy, to reflect organisational or geographical structure, or to partition the security management in order to cope with the complexity of large distributed systems.

An access control policy specifies, in terms of domains, what operations a set of subjects is permitted to perform on a set of targets. In a distributed system, however, a client often delegates access rights to a proxy server to perform operations on behalf of the client. As delegation of access rights should be controlled, the notion of the access control policy has been extended to deal with cascaded delegation.

The security architecture provides a high degree of access control and authentication transparency to the application level by utilising security agents on each host. A policy dissemination mechanism has been developed to propagate policies through hierarchical domain structures to the agents of the concerned objects and deal with changes in the domain structure.

The access control mechanism, which is based on the Access Control List (ACL) paradigm, enforces access control policies specified in terms of domains and deals with cascaded delegation of access rights.

As the access control decisions are based on domain membership, there is a need to efficiently authenticate domain membership as well as object and user identity. The proposed intra-realm authentication system is based on symmetric cryptography to minimise the encryption/decryption overhead. Verification of domain membership is based on statements issued by the domain service and translated by the authentication system into the keys of the verifiers. Similarly, verification of delegation is based on delegation tokens issued by the grantors and translated into the keys of the end-points.

Document téléchargé depuis www.pnst.cerist.dz CERIST

ΣΤΟΥΣ ΓΟΝΕΙΣ ΜΟΥ
ΓΕΩΡΓΙΟ ΚΑΙ ΚΩΝΣΤΑΝΤΙΝΑ
(To my parents George and Constantina)

Acknowledgements

I am indebted to my supervisor Professor Morris Sloman. This work would not have been carried out without his guidance, suggestions and constructive criticism. My thanks are also due to Dr Jonathan Moffett, Dr Kevin Twidle, Damian A. Marriott and Emil Lupu who took time to read reports describing earlier stages of this work and provided useful feedback.

I also wish to acknowledge the help given me by many research students, research assistants and others members of the Distributed Software Engineering Section. Thank you Paris Bayias, S.C. Cheung, Paul Dias, Douglas Donaldson, Naranker Dulay, Hal Fossa, Dimitra Giannakopoulou, Celso Hirata, Christos Karamanolis, Masoud Mansouri-Samani, Nabor das Chagas Mendonca, Kaveh Moazami-Goudarzi, Keng Ng, Wai Leung Poon, Thanwadee Thanitsukkarn and Andrea Zisman.

My thanks are also due to Tracy Banton, Aspassia Daskalopoulou, Kostis Dryllerakis, Monica Leutner, Fotini G. Markopoulou-Kalamara, Stavros Menegos, Anne O'Neill, Yongyuth Permpoontanalarp and Nikos Scarmeas, who all have contributed considerable help during my studies at Imperial College.

I gratefully acknowledge financial support from the British Council, Swiss Bank Corporation (London), Esprit SysMan (7026) Project and Imperial College.

Document téléchargé depuis www.pnst.cerist.dz CERIST

Table of Contents

Table of Contents vii
List of Figures xiii
List of Tables xvii
List of Abbreviations xix

Chapter 1

Introduction 21
1.1 Motivation and Aims 21
1.2 Our Approach 24
1.3 What is New in this Thesis 25
1.4 Thesis Outline 26

Chapter 2

Background 29
2.1 Security in Distributed Systems 29
2.1.1 Information Security 30
2.1.2 Threats in a Distributed System 30
2.1.3 Security Functionality 31
2.2 Access Control Policy 32
2.2.1 Security Policy 32
2.2.2 Access Control Policy 33
2.2.3 Traditional Access Control Policies 34
2.3 Access Control Enforcement 35
2.3.1 Reference Monitor 35

2.3.2 Access Control Lists and Capabilities 36
2.3.3 An Access Control Calculus 38
2.4 Basic Cryptographic Tools 41
2.4.1 An Example 41
2.4.2 Symmetric Cryptography 42
2.4.3 Symmetric Cryptosystems 43
2.4.4 Asymmetric Cryptography 45
2.4.5 Asymmetric Cryptosystems 46
2.4.6 Hash Functions 47
2.4.7 Message Authentication Code (MAC) 47
2.4.8 Ensuring Message Secrecy and Integrity 48
2.4.9 Cryptanalysis 49
2.5 Authentication 51
2.5.1 Basic Aspects 51
2.5.2 Authentication Based on Symmetric Cryptography 53
2.5.3 Authentication Based on Asymmetric Cryptography 54
2.5.4 Relays 55
2.5.5 Multiple Authentication Servers and CAs 56
2.5.6 Other Authentication Issues 57
2.6 Chapter Summary 57

Chapter 3

Domain-Based Access Control 59
3.1 The Domain Concept 59
3.1.1 Objects 60
3.1.2 Domains 60
3.1.3 Domain Service 62
3.2 Domain-Based Policies 62
3.2.1 The Principle 63
3.2.2 Domain Scope Expressions 64
3.2.3 Access Rules 66
3.2.4 Policies Applying to Users 69
3.2.5 Policy Service 70
3.2.6 Authorisation Policies for Security Administrators 70
3.2.7 Roles 71
3.3 Chapter Summary 72

Document téléchargé depuis www.pnst.cerist.dz CERIST

Chapter 4

Delegation of Access Rights 73
4.1 Introduction 73
4.1.1 The Problem 74
4.1.2 Some Definitions 75
4.1.3 Cascaded Delegation 76
4.1.4 Discussion.. 76
4.2 Related Work 77
4.2.1 General 78
4.2.2 Delegation in Taos.. 79
4.3 Extended Access Rules 84
4.3.1 Controlling Delegation in Distributed Systems 84
4.3.2 Extended Access Rules 84
4.3.3 An Example 87
4.4 Chapter Summary 89

Chapter 5

Overview of the Security Architecture 91
5.1 Introduction 91
5.2 Access Control... 93
5.3 Authentication System 95
5.3.1 Registration of Principals.. 95
5.3.2 Verification of Domain Membership 96
5.3.3 Delegation 96
5.3.4 User Authentication 97
5.4 Secure Channels... 98
5.4.1 A Typical Scenario 98
5.5 Related Work 101
5.7 Chapter Summary 103

Document téléchargé depuis www.pnst.cerist.dz CERIST

Chapter 6

Access Control 105
6.1 Introduction 105
6.2 Policy Distribution...106
6.2.1 Dynamic Policy Scopes...106
6.2.2 Propagation of Policy Scope Evaluation Tokens (PETs)..................107
6.2.3 Dynamic Domain Structures..110
6.2.4 Monitoring the Propagation Process 111
6.2.5 Policy Hand Over...112
6.3 Propagation of Pseudo-Capabilities 113
6.3.1 Determination of the Pseudo-Capability Certificate Sets...................114
6.3.2 Special Cases..116
6.4 Secure Channel Access Control Information.................................116
6.4.1 Access Control Information Held by the ACAs............................116
6.4.2 Determining the Privileges of the Subject..................................118
6.4.3 One-Hop Delegation..121
6.4.4 Cascaded Delegation 122
6.5 Restricted Access Rights...124
6.5.1 An Example 124
6.5.2 Pseudo-Capability Select Expressions 126
6.5.3 Restriction of Rights by a Grantee..128
6.6 Access Control API 128
6.6.1 The Interface 128
6.6.2 An Example 130
6.7 Chapter Summary 133

Chapter 7

Authentication System 135
7.1 Introduction 135
7.2 Asymmetric vs. Symmetric Cryptography 136
7.2.1 Asymmetric cryptography 136
7.2.2 Symmetric cryptography...138
7.3 Authentication Servers with Minimal State 138
7.3.1 Private-Key Certificates..138

Document téléchargé depuis www.pnst.cerist.dz CERIST

7.3.2 Basic Aspects and Notation 139
7.3.3 Establishing Shared Keys Between Authentication Agents 140
7.3.4 Translation of Messages 142
7.3.5 Certificate Revocation 144
7.4. Secure Channels 146
7.4.1 Communication Security 146
7.4.2 Channel Keys 147
7.4.3 Setting up a Secure Channel 148
7.4.4 Cryptographic Facilities 149
7.5. Verification of Domain Membership 150
7.5.1 An Example 151
7.5.2 Domain Membership and Secure Channels 153
7.6 Delegation of Access Rights 153
7.6.1 Delegation Protocols 154
7.6.2 Revocation of Delegation Tokens 158
7.6.3 Restricted Access Rights 158
7.6.4 Discussion and Related Work 159
7.7 Chapter Summary 161

Chapter 8

Conclusions 163
8.1 Review of Aims and Accomplishments 163
8.1.1 Delegation of Access Rights 164
8.1.2 Policy Distribution 165
8.1.3 Access Control Enforcement 165
8.1.4 Authentication 166
8.1.5 Security Architecture 167
8.2 Performance Issues 167
8.2.1 Usage Assumptions 167
8.2.2 Numerical Estimates 168
8.2.3 Pull vs. Push 173
8.3 Further Work 174
8.4 Final Remarks 175

Document téléchargé depuis www.pnst.cerist.dz CERIST

Appendix

Evaluation of Policy Scopes **177**
A.1 Propagation Control Flags (PCFs) 177
A.1.1 Controlling the Propagation Depth 178
A.2 Policy Scope Evaluation Tokens (PETs) 179
A.2.1 Skeleton Parser 181
A.2.2 An Example 182
A.3 Dynamic Domain Structure 184
A.3.1 Insertion of a Non-Domain Object 185
A.3.2 Removal of a Non-Domain Object 185
A.3.3 Insertion of a Subdomain 186
A.3.4 Removal of a Subdomain 187
A.4 Policy Retraction 187
A.5 Propagation in the Subject and Grantee Scopes 187

Bibliography **191**

Document téléchargé depuis www.pnst.cerist.dz CERIST

List of Figures

Figure 1.1 Main Issues Discussed in This Thesis 24
Figure 2.1 Security Functionality and Dependencies.................................... 32
Figure 2.2 ISO Reference Monitor 35
Figure 2.3 Example for Multiple Reference Monitors.................................. 36
Figure 2.4(a) Use of Access Control Lists 37
Figure 2.4(b) Use of Capabilities.. 37
Figure 2.5 An Example for Cryptographically Protected Communication............. 42
Figure 2.6 Use of a Message Authentication Code (MAC).............................. 48
Figure 2.7 Encryption of a Message Along With its Digest 49
Figure 2.8 Kerberos V4 Authentication Protocol (simplified).......................... 53
Figure 3.1 Object Identifier.. 60
Figure 3.2 Two Graphical Representations of a Domain Structure..................... 61
Figure 3.3 Domain Service Provided by Multiple Domain Servers..................... 63
Figure 3.4 A Domain Structure 65
Figure 3.5 Policy Refinement and Enforcement 67
Figure 3.6 Graphical Representation of an Access Rule 68
Figure 3.7 Adapter Object Acting on behalf of a User 69
Figure 3.8 Administrator Interacting with the Policy Service 70
Figure 3.9 Authorisation Policy for a Security Administrator (SA) 71
Figure 4.1 A Tree of Cascaded Invocations 74
Figure 4.2 A Cascaded Invocation Scenario.. 75
Figure 4.3 Cascaded Delegation 76
Figure 4.4 Sketch of the Delegation Issue 77
Figure 4.5 One-hop Delegation 80
Figure 4.6 Two-Hop Delegation... 82
Figure 4.7 Graphical Representation of an Extended Access Rule 85
Figure 4.8 Cascaded Delegation Permitted by an Extended Access Rule 86
Figure 4.9 Partial View of an Hypothetical Domain Structure 88
Figure 4.10 Cascaded Delegation Controlled by the Rules in Table 4.1 89
Figure 5.1 Sketch of the Security Architecture... 93

Document téléchargé depuis www.pnst.cerist.dz CERIST

Figure 5.2 Dissemination of Access Rules (simplified) 94
Figure 5.3 A Possible Membership Path 97
Figure 5.4 Subject Host and Secure Channel Establishment 99
Figure 5.5 Target Host and Secure Channel Establishment........ 100
Figure 6.1 Three States of a Domain Structure 107
Figure 6.2 Two-phase Policy Dissemination 108
Figure 6.3 An Example of PCF Propagation 109
Figure 6.4(a) Example for PET Propagation When Insertion of a Subdomain Takes Place 110
Figure 6.4(b) Example for PET Propagation When Removal of a Subdomain Takes Place 110
Figure 6.5 Propagation of Acknowledgements........ 111
Figure 6.6 Reporting a Propagation Failure 113
Figure 6.7 Policy Hand Over and Retraction 114
Figure 6.8 Propagation in the Subject Scope and Determination of the Capability Certificate Set (CCS) 115
Figure 6.9 Access Control Information Held by an ACA 117
Figure 6.10 Construction of the Candidate Channel Policy List 118
Figure 6.11 Construction of the RCPL........ 119
Figure 6.12 Construction of the CCPL for One-Hop Delegation 120
Figure 6.13 Construction of the RCPL When Delegation Takes Place 122
Figure 6.14 Cascaded Delegation 123
Figure 6.15 Example for Restriction of Access Rights 125
Figure 6.16 Example for Pseudo-Capability Select Expressions 127
Figure 6.17 Cascaded Delegation Controlled by the Rules in Table 4.1 132
Figure 7.1 Using Private Key Certificates to Disperse the Security Database 139
Figure 7.2 Shared secret key establishment between authentication agents 141
Figure 7.3 Message Translation by the Authentication Service........ 143
Figure 7.4 Translation of a CRL 144
Figure 7.5 Authentication Agents Setting Up a Secure Channel 148
Figure 7.6 Invocation on a Channel Providing Authenticity and Secrecy 150
Figure 7.7 Example of Domain Membership Verification........ 152
Figure 7.8 One Step Delegation Protocol 155
Figure 7.9 Two Step Delegation Protocol........ 156
Figure 7.10 Misuse of Delegation Token if the PDT Field is Omitted 157
Figure 7.11 Attack on the Delegation Protocol Using Repeated DIDs........ 157
Figure 7.12 Revocation of a Delegation Token........ 158
Figure A.1 Propagation of a PCF 179
Figure A.2 Propagation of Two PCFs Generated by *DomA - *DomB 180

Document téléchargé depuis www.pnst.cerist.dz CERIST

Figure A.3 Propagation of PETs by *DomA - (*2DomB ^ @DomC) 183
Figure A.4 Propagation of PCFs by *DomA - (*2DomB ^ @DomC) 184
Figure A.5(a) Example for Insertion of a Subdomain 186
Figure A.5(b) Example for Removal of a Subdomain.................................... 186
Figure A.6 Propagation of PCFs in Negative PETs for Policy Retraction............. 188
Figure A.7(a) Propagation of PCFs in the Subject Scope of *A 189
Figure A.7(b) Removal of a PCF 189

Document téléchargé depuis www.pnst.cerist.dz CERIST

List of Tables

Table 2.1 DES Modes of Operation.. 44
Table 4.1 A Set of Extended Access Rules 88
Table 5.1 Distribution of Information Related to a Secure Channel........................ 100
Table 8.1 Estimated Invocation Latency on Secure Channels 169
Table 8.2 Numerical Estimates using Symmetric and Asymmetric Cryptosystems....... 171
Table 8.3 Delegation-related Estimates using Symmetric and Asymmetric Cryptosystems.. 172
Table A.1 Skeleton Parser States.. 185

Document téléchargé depuis www.pnst.cerist.dz CERIST

Document téléchargé depuis www.pnst.cerist.dz CERIST

List of Abbreviations

AA	Authentication Agent
ACA	Access Control Agent
ACPL	Access Control Policy List
AR	Access Rule
AS	Authentication Service
CA	Certification Authority
CCPL	Candidate Channel Policy List
CCS	Capability Certificate Set
CF	Cryptographic Facility
CHID	Secure Channel Identifier
CID	Certificate Identifier
CRL	Certificate Revocation List
DAR	Delegated Access Rights
DID	Delegation token Identifier
DMCL	Delegation Membership Certificate Set
DPCL	Delegation Pseudo-Capability List
DRL	Delegation token Revocation List
DSE	Domain Scope Expression
DSSA	Distributed Systems Security Architecture
DT	Delegation Token
GCCS	Grantee Capability Certificate Set
GPCL	Grantee Pseudo-Capability List
MAC	Message Authentication Code
OID	Object Identifier
OMG	Object Management Group
ORB	Object Request Broker
PCF	Propagation Control Flag
PCL	Pseudo-Capability List
PDT	Preceding Delegation Token
PET	Policy scope Evaluation Token
PFS	Perfect Forward Security
PKC	Private-Key Certificate
PSCE	Pseudo-Capability Select Expression
RCPL	Resolved Channel Policy List
RMF	Reference Monitor Facility
RPD	Role Position Domain
SMCL	Subject Membership Certificate List
SN	Serial Number
TCB	Trusted Computing Base
UID	Unique Identifier
URD	User Representation Domain