Break-Glass

Helmut Petritsch

Break-Glass

Handling Exceptional Situations in Access Control

With a Foreword by Prof. Dr. Günther Pernul

Springer Vieweg

Dr. Helmut Petritsch
Walldorf, Germany

Dissertation, University of Regensburg, 2014

ISBN 978-3-658-07364-0 ISBN 978-3-658-07365-7 (eBook)
DOI 10.1007/978-3-658-07365-7

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Library of Congress Control Number: 2014950445

Springer Vieweg

© Springer Fachmedien Wiesbaden 2014
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law. The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use. While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer Vieweg is a brand of Springer DE.
Springer DE is part of Springer Science+Business Media.
www.springer-vieweg.de

Foreword

Break-glass is a mechanism to handle exceptional situations in access control. Under emergency situations users should be able – to a certain extent – to request exceptional privileges to achieve tasks which could not be accomplished otherwise. Afterwards, after the emergency situation has been resolved, authorities responsible for auditing a security policy should be able to check if the exceptional access can be justified.

In this book the author develops a break-glass concept which is orthogonal to existing access control techniques. As such, the break-glass does not rely on specific properties of a given access control model. This is in contrast to other approaches which mainly try to integrate exception-handling into a particular access control model. Grounded on requirements stemming from real-world application cases and legal requirements, the author develops a comprehensive generic break-glass model consisting of a three-step process: pre-access, at-access, and post-access. Each of the process steps is thoroughly analyzed and the major components and players identified. In addition, much effort is devoted to the post-access break-glass analysis with the focus on developing an analysis infrastructure in order to support validity checks and perform the auditing of the exceptional access. All the findings of the author are evaluated and partly tested by a prototype implementation under almost real-world conditions.

In addition to break-glass, this book also describes state-of-the-art achievements in a wider range of topics, such as authorization systems, XACML-based authorization policies, role-based access control systems, software architectures and the form of their representation. The focus of the book is on the technical and organizational issues. This book is mainly recommended for readers who are interested in its valuable contributions to research, but also for those looking for a comprehensive summary of the state of the art of break-glass and related technologies.

Prof. Dr. Günther Pernul
Department of Information Systems
University of Regensburg, Germany

Contents

1 Introduction **1**
1.1 Motivation 1
1.2 Running Example 6
1.2.1 Regular Use Case 6
1.2.2 Break-Glass Use Case 8
1.2.3 Post-Access Investigations 11
1.3 Methodology 11
1.4 Thesis Structure 13

2 Background **15**
2.1 Information Security 15
2.2 Access Control 18
2.2.1 Concepts 18
2.2.2 Access Control Models 21
2.2.3 Distributed Access Control Systems 29
2.2.4 XACML 31

3 A Generic Break-Glass Model **37**
3.1 Requirements of Break-Glass 37
3.2 Abstract Model 41
3.3 Core Model 43
3.4 Constraints Model 45

4 Policy Definition: Pre-Access **51**
4.1 Authorization Infrastructure 51
4.1.1 Break-Glass Architecture 51
4.1.2 Policy Permissions and Policy State 53
4.1.3 Policy State Administration 59
4.1.4 Policy Language 66
4.1.5 Expressing Regular Privileges for Healthcare 68
4.2 Break-Glass Policies 74
4.2.1 Policy Structure 75

4.2.2 Modeling Break Glass 77
4.2.3 Stateful Break-Glass 78
4.2.4 Constraints Model in XACML 85
4.3 Expressing Exceptional Privileges 88

5 User Information: At-Access 93
5.1 Override Measurement 93
5.1.1 Information Sources 95
5.1.2 Merging Algorithms 97
5.1.3 Identifying Mentors 99
5.2 Recording the System State 101
5.2.1 Versioning System State and Security State 101
5.2.2 Logging Break-Glass Accesses 102
5.2.3 Recording At-Access Information 103

6 Analysis: Post-Access 107
6.1 Post-Access Break-Glass Analysis 107
6.2 Analysis Infrastructure 111
6.2.1 Authorization Infrastructure 111
6.2.2 PDP Analysis Extension 114
6.3 Policy-Driven Analysis 120
6.3.1 Automated Analysis with Post-Access Information . . 121
6.3.2 Preserving Analysis Knowledge 122

7 Implementation 125
7.1 Break-Glass Landscape 125
7.2 Analysis Workbench 131

8 Related Work 137
8.1 Pre-Staging Emergency Accounts and Roles 138
8.2 Categorization of Permissions 139
8.3 Break-Glass Models 147
8.3.1 Post-Access Models 147
8.3.2 RBAC Extensions 149
8.3.3 Process-Based Approaches 152
8.3.4 Multi-Level Security Adoptions 155
8.3.5 Delegation-Based Models 157
8.3.6 XACML-Based Approaches 159
8.4 Field Tests 161

9 Evaluation 165

9.1 Requirements vs. Properties 165
9.2 Classification of Break-Glass 167
9.3 Generalized Break-Glass Models 169

10 Discussion and Conclusion 177

10.1 Contributions 177
10.2 Research Questions 178
10.3 Discussion 182
10.3.1 Properties of the Break-Glass Model 182
10.3.2 Applications of the Break-Glass Model 187
10.3.3 Obligations vs. Third Access Control Decision 189
10.3.4 Non-Overridable DENY Decisions vs. Constraints . . 191
10.3.5 Possible Model Variants 192
10.4 Future Work 194
10.5 Conclusion 195

Bibliography 197

A Glossary 209

B Acronyms 211

C Code Samples 215

C.1 XACML Sample Policy 215
C.2 Lattice Evaluation Algorithm in Java 217

List of Figures

2.1 Core RBAC 23
2.2 Sequence Diagram: Granted Request 30
2.3 Distributed Security Architecture 31

3.1 Break-Glass Lifecycle 38
3.2 Break-Glass Policy Lattice 42
3.3 Policy Lattice with DENY Policies 46

4.1 Break-Glass Architecture 52
4.2 Sequence Diagram: User Confirmed Break-Glass Access . . . 53
4.3 Sequence Diagram: User Canceled Break-Glass Access 54
4.4 Data-Flow in an Authorization Infrastracture 57
4.5 Sequence Diagram: Policy State Usage 61

6.1 Analysis Workbench Architecture 112

7.1 Class Diagram: Policy State Implementation 127
7.2 Class Diagram: Log Server Implementation 130

10.1 Policy Lattice Restricting Regular Access 188

List of Listings

2.1 Reduced XACML Represenation: Sample Policy 34

3.1 Lattice Evaluation Algorithm: Core Model 44
3.2 Naive Lattice Evaluation Algorithm: Constraints Model . . . 47
3.3 Improved Lattice Evaluation Algorithm 48

4.1 Policy State Policy 62
4.2 Policy State Assignment 65
4.3 XACML Variable Definitions 71
4.4 Positive Permissions for Nurse and Physician 72
4.5 Regular Poliy for Patient Data 74
4.6 Policy Structure 76
4.7 Activation of Policies as Policy State Dependency 78
4.8 Stateful Break-Glass: Policy State Dependency 81
4.9 Stateful Break-Glass Policy 81
4.10 Policy Lattice with DENY Policies 87

5.1 XACML Policy: Recording At-Access Information 104

6.1 Reduced Policy by Means of a Concrete Request 115
6.2 Abstract Evaluation 117
6.3 Time-In-Range Function for HOL-TESTGEN 119
6.4 Post-Access Policy for Automated Analysis 123

7.1 Analysis Modifications to the XACML Implementation 133

C.1 XACML Sample Policy 215
C.2 Lattice Evalution Algorithm in Java 217