Adaptive Cryptographic Access Control

Advances in Information Security

Sushil Jajodia
Consulting Editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

For other titles published in this series, go to
www.springer.com/series/5576

Anne V.D.M. Kayem • Selim G. Akl
and Patrick Martin

Adaptive Cryptographic Access Control

Foreword by Sylvia L. Osborn

Springer

Anne V.D.M. Kayem,
Department of Computer Science,
University of Cape Town,
Private Bag X3, 18 University Ave.,
Rondebosch 7701,
Cape Town, South Africa.
akayem@cs.uct.ac.za

Selim G. Akl,
School of Computing,
Queen's University,
Kingston, Ontario,
K7L 3N6, Canada.
akl@cs.queensu.ca

Patrick Martin,
School of Computing,
Queen's University,
Kingston, Ontario,
K7L 3N6, Canada.
martin@cs.queensu.ca

ISSN 1568-2633
ISBN 978-1-4419-6654-4 e-ISBN 978-1-4419-6655-1
DOI 10.1007/978-1-4419-6655-1
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2010932005

© Springer Science+Business Media, LLC 2010
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.
The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To our beloved ones for being so supportive and patient, even the during trying moments.

Foreword

For a designer of the security for an information system, a large number of concepts must be mastered, not to mention the interactions of these concepts with each other. Should I use cryptography? How do I generate keys? How do I change keys if I think my system has been breached? Do I have to re-encrypt all my data every time I generate a new key for one class of data? Do I have to be constantly monitoring the system and intervening to update keys?

This monograph provides answers to all of these questions. It begins by presenting thorough background on access control models in general and, in more detail, on cryptographic access control. The assumption is made that keys will be assigned to groups, so that when the security policy gives a group access to some data, the key can be used for decryption of the data that is to be visible to the group. An algorithm, which improves on previous techniques, for minimizing the cost of key assignment and replacement is presented, and analysed both theoretically and with experiments. A further improvement to the time taken for re-keying is also presented.

If the security policy changes frequently, group memberships may change, requiring both new keys and re-encrypting the data accessible to the group. The techniques mentioned above reduce the time for rekeying and re-encryption over existing techniques. To cope with a high frequency of changes, an autonomic computing model is used to create an adaptive rekeying approach to key management, thus freeing the security administrator from some of their monitoring load. Finally, the implications of managing encrypted data when it is stored on a third-party site are also discussed.

The monograph, while scholarly, is written in manner that makes it readable by both practitioners and researchers. It combines a solid theoretical approach with experimental evaluation, so that the user of these new algorithms and techniques can be assured not only that they will work, but also that they will be more efficient that previous approaches.

London, Ontario, Canada; March, 2010 *Sylvia L. Osborn*

Preface

Our motivations for writing this monograph are centered on the fact that although a significant amount of research exists on the topics of cryptographic key management and access control, most texts tend to focus on access control models and only cover cryptographic key management superficially. This monograph is meant to help students, researchers, and teachers with an interest in access control and cryptographic key management. For the student, our purpose is to present material in a readable manner, and highlight the current trends in cryptographic key management. Our goal was to show students, who are often skeptical about the practicality of cryptographically supported access control, how access control and cryptographic key management can be combined to ensure data security.

For the researcher, our goal is to analyze the different solutions that have been presented in the literature highlighting their pros and cons with respect to the growing need for adaptive security. We go on to present a method of implementing adaptive access control and discuss the challenges involved in designing adaptive access control schemes. It is our hope that we have achieved our goal of kindling interest in this area by evoking some of the interesting problems worth working on.

For the instructor, this text will serve as support material for the topics of cryptographic key management and access control. We hope that it will give instructors a broader and in depth perspective of both topics allowing them to teach more effectively and efficiently in ways that are most appropriate for their particular set of students.

Acknowledgements

We would like to gratefully acknowledge the people that have directly or indirectly contributed to the content of this monograph by kindly providing several helpful comments and pointing out typographical errors that helped improve the quality of the work presented. Among them, Sylvia Osborn, Stafford Tavares, Mohammad Zulkernine, and Hagit Shatkay. In spite of these contributions, there may still be er-

rors in the monograph and we alone must take responsibility for those. We are also deeply indebted to the Canadian Commonwealth Scholarship Fund for fnancially supporting the research on which this text is grounded.

Bremen, Germany; *Anne V.D.M. Kayem*
Kingston, ON, Canada; March, 2010 *Selim G. Akl, and Patrick Martin*

Contents