

Automated Security Management

Ehab Al-Shaer • Xinming Ou • Geoffrey Xie
Editors

Automated Security Management

Editors

Ehab Al-Shaer
Department of Software and
Information Systems
University of North Carolina Charlotte
Charlotte, NC, USA

Xinming Ou
Computing and Information Sciences
Kansas State University
Manhattan, KS, USA

Geoffrey Xie
Department of Computer Science
Naval Postgraduate School
Monterey, CA, USA

References to various copyrighted trademarks, servicemarks, marks and registered marks owned by the respective corporations and/or connected subsidiaries may appear in this book. We use the names, logos, and images only in an editorial fashion with no intention of infringement of the trademark.

ISBN 978-3-319-01432-6 ISBN 978-3-319-01433-3 (eBook)
DOI 10.1007/978-3-319-01433-3
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013947169

© Springer International Publishing Switzerland 2013

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

Preface

With the increasing trend of cyber attacks, more security technologies and devices have been developed. A typical enterprise network might have hundreds of security devices such as firewalls, IPSec gateways, IDS/IPS, authentication servers, authorization/RBAC servers, and crypto systems. However, each security device might contain thousands of security configuration variables and rules that must be set correctly and consistently across the entire network in order to enforce end-to-end security properties. Moreover, security configuration must be constantly changing to optimize protection and block prospective attacks. Tuning configuration to balance security, flexibility, and performance is another major challenging task. This is extremely burdensome not only for regular users but also for experienced administrators, who have to be very lucky to get things working right all the time. The resulting security configuration complexity places a heavy burden on both regular users and experienced administrators and dramatically reduces overall network assurability and usability.

Automated Security Management presents a number of topics in the area of configuration automation. This book is based on papers published at the fifth Symposium on Configuration Analytics and Automation (SafeConfig 2012). It is a source of information for IT security configuration automation for both researchers and practitioners. Part I introduces modeling and validation of configurations based on high-level requirements. Part II discusses how to manage the security risk as a result of configuration settings of network systems. Part III introduces the concept of configuration analysis and why it is important in ensuring the security and functionality of a properly configured system. Part IV presents ways to identify problems when things go wrong. We would like to thank all the chapter authors for contributing such a diverse collection of timely and interesting research results.

Charlotte, NC, USA
Manhattan, KS, USA
Monterey, CA, USA

Ehab Al-Shaer
Xinming Ou
Geoffrey Xie

Contents

Part I Configuration Modeling and Checking

1	Towards a Unified Modeling and Verification of Network and System Security Configurations	3
	Mohammed Noraden Alsaleh, Ehab Al-Shaer, and Adel El-Atawy	
2	Modeling and Checking the Security of DIFC System Configurations	21
	Mingyi Zhao and Peng Liu	

Part II Vulnerability and Risk Assessment

3	Increasing Android Security Using a Lightweight OVAL-Based Vulnerability Assessment Framework	41
	Martín Barrère, Gaëtan Hurel, Rémi Badonnel, and Olivier Festor	
4	A Declarative Logic-Based Approach for Threat Analysis of Advanced Metering Infrastructure	59
	Mohammad Ashiqur Rahman and Ehab Al-Shaer	
5	Risk Based Access Control Using Classification	79
	Nazia Badar, Jaideep Vaidya, Vijayalakshmi Atluri, and Basit Shafiq	

Part III Configuration Analytics

6	GCTNav: Generic Configuration Navigation System	99
	Shankaranarayanan Puzhavakath Narayanan, Seungjoon Lee, and Subhabrata Sen	

7	The Right Files at the Right Time	119
	Hayawardh Vijayakumar and Trent Jaeger	
8	Rule Configuration Checking in Secure Cooperative Data Access....	135
	Meixing Le, Krishna Kant, and Sushil Jajodia	
 Part IV Diagnostics and Discovery		
9	Programmable Diagnostic Network Measurement with Localization and Traffic Observation	153
	Michael R. Clement and Dennis Volpano	
10	Discovery of Unexpected Services and Communication Paths in Networked Systems	169
	Ichita Higurashi, Akira Kanaoka, Masahiko Kato, and Eiji Okamoto	
11	Tracing Advanced Persistent Threats in Networked Systems	179
	Masahiko Kato, Takumi Matsunami, Akira Kanaoka, Hiroshi Koide, and Eiji Okamoto	