Automated Security Management

Ehab Al-Shaer • Xinming Ou • Geoffrey Xie
Editors

Automated Security Management

Springer

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

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

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 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 — Ehab Al-Shaer
Manhattan, KS, USA — Xinming Ou
Monterey, CA, USA — Geoffrey Xie

Contents