Dynamic Secrets in Communication Security

Sheng Xiao · Weibo Gong
Don Towsley

Dynamic Secrets in Communication Security

Springer

Sheng Xiao
College of Information Science
and Engineering
Hunan University
Changsha, Hunan
People's Republic of China

Weibo Gong
Department of Electrical and Computer
Engineering
University of Massachusetts Amherst
Amherst, MA
USA

Don Towsley
Department of Computer Science
University of Massachusetts Amherst
Amherst, MA
USA

ISBN 978-1-4614-7830-0 ISBN 978-1-4614-7831-7 (eBook)
DOI 10.1007/978-1-4614-7831-7
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2013942180

Printed on acid-free paper

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

Preface

This book introduces *dynamic secrets* as a new approach for cryptographic key management in secure communication systems. This approach allows a stolen cryptographic key to be automatically recovered shortly after the incidence of key theft. It also provides an intrinsic mechanism to promptly detect *all* active attacks using a stolen key.

Dynamic secrets complement and expand Kerckhoffs' principle, a guideline for cryptosystem design since the nineteenth century. Kerckhoffs' principle asserts that security of a cryptosystem should solely rely on the secrecy of its key. In this monograph, we demonstrate that dynamic secrets can constantly "refill" key secrecy during the communication process. Therefore, a secure communication system can remain functional even if its key is known to an adversary.

The intended audiences of this book include researchers, professionals, graduate and undergraduate students with interests in communication security. In order to rigorously analyze security properties provided by dynamic secrets, this book contains ideas from information theory and probability theory. We put efforts in writing to ensure that readers who are unfamiliar with these disciplines can perceive the entire scope of dynamic secrets, and implement dynamic secrets in practical secure communication systems after reading this book.

Amherst, MA, USA, January 2013

Sheng Xiao
Weibo Gong
Don Towsley

Acknowledgments

The author Sheng Xiao thanks the other two authors, Prof. Weibo Gong and Prof. Don Towsley for their mentorship and support throughout his Ph.D. years. Without them, the dynamic secrets research would be impossible. He would also like to thank Prof. Dennis Goeckel and Prof. Hossein Pishro-Nik in University of Massachusetts, Amherst, Prof. Robert Gao in University of Connecticut, Storrs, Prof. Jie Wang in University of Massachusetts, Lowell, and Prof. Xiaohong Guan in Xian Jiaotong University, China, for their helpful discussions and encouragements for the research. He also wishes to thank Dr. Roberto Padovani and Prof. Jack Wolf for their encouragement when they visited UMASS.

The author Weibo Gong thanks Prof. Michael Rabin whose work on everlasting security motivated the initial thought on using channel randomness for security. He would also like to thank Prof. David M. Pozar for the early discussions on channel randomization for secure wireless communications.

All three authors thank the United States National Science Foundation for their support of grants EFRI-0735974, CNS-1065133, CNS-1239102, and CNS-1018464, the Army Research Office for their support of contract W911NF-08-1-0233, and the University of Massachusetts for their support of the CVIP Technology Award Fund.

Contents