

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

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

Weibo Gong
Department of Electrical and Computer
Engineering
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

© Springer Science+Business Media New York 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 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

1	Introduction	1
2	Communication Security and Key Safety	5
2.1	Secure Communication System Design and Locksmith	5
2.2	Challenges to Ensure Key Safety	8
2.2.1	Key Cracking	8
2.2.2	Key Stealing	10
3	Dynamic Secrets	13
3.1	Dynamic Key Preview	14
3.2	Dynamic Secrets in Noisy Packet Communications	15
3.2.1	Noisy Packet Communication Model	15
3.2.2	Dynamic Secrets and Dynamic Key	16
3.3	True Randomness at Low Cost	18
3.3.1	Efficiency of True Randomness Harvest	20
3.4	Automatic Stolen Key Recovery	22
3.4.1	Rate of the Stolen Key Recovery	24
3.5	Inherent Detection to Impersonation Attack	26
3.5.1	Detect Impersonation Attack Without False Alarm	29
3.5.2	Man-in-the-Middle Attack	32
4	Dynamic Wireless Security	33
4.1	Stop-and-Wait (SW) Protocol	34
4.2	Dynamic Secrets in the Wireless LAN Link Layer	35
4.2.1	Automatic Frame Classification	36
4.2.2	Dynamic Secrets Generation	39
4.2.3	Dynamic Key Updates	39
4.3	Proof-of-Concept Experiments	41
4.3.1	Prototype Design	42
4.3.2	Experiments on Computational Complexity	44
4.3.3	Experiments on Adversary's Information Loss	46
4.3.4	Experiments on Environmental Randomness	48

4.4	Dynamic Secrets in Other Layers of Wireless Communications	49
4.4.1	Throughput Efficient Implementation in Network Layer	49
4.4.2	Application Layer Dynamic Secrets, Leasing and Proxying	51
5	Dynamic Key Management in a Smart Grid	55
5.1	Smart Grid and Cryptographic Key Management	56
5.1.1	Traditional Key Management Schemes and Challenges	58
5.2	Dynamic Key, a Node-to-Node Autonomy	60
5.2.1	Key Updates Between Meter and Collector	60
5.2.2	Security Properties of Dynamic Key Updates	63
5.2.3	Computation, Storage, and Bandwidth Cost	64
5.3	Node Installation, Node Removal, and Trust Propagation	65
5.3.1	Node Installation and Removal	65
5.3.2	Trust Propagation and End-to-End Secure Communication	66
5.4	Scalability and Crisis Response	67
6	Secrecy in Communications	69
6.1	Adversary's Unknown Information and Secrets	70
6.1.1	Traditional Symmetric Key	73
6.1.2	Asymmetric Key	73
6.1.3	Dynamic Secrets and Dynamic Key	74
6.1.4	Man-in-the-Middle Adversary with Key	75
6.2	Universal Hashing and Secrecy Extraction	76
6.2.1	Secrecy Extraction Efficiency	76
6.2.2	Deterministic Hashing and Mixed, Imperfect Secret	78
6.2.3	Secrecy Extraction in Small Time Segments	79
6.3	Quantum Key Distribution and Dynamic Key	80
6.3.1	QKD in a Dynamic Secrets View	80
6.3.2	Dynamic Secrets as Low Cost QKD	81
6.3.3	Long Distance Key Establishment	83
6.4	Secrecy Sharing, Perfect Secret, and Dynamic Secrets	83
6.4.1	Secrecy Sharing Problem	83
6.4.2	Non-decreasing Key Secrecy	84
6.4.3	Perfect Secret	86
6.4.4	Asymptotic One Time Pad	86
6.5	Error Detectable but Non-correctable Codes	87

- 7 Reliability Analysis for Communication Security** 91
 - 7.1 Reliability Theory Preliminaries 92
 - 7.2 Key Safety as a Reliability Problem 94
 - 7.2.1 Reliability Properties in Communication Security Context 95
 - 7.2.2 Poisson Process Modeling of Key Thefts 95
 - 7.3 Reliability Analysis for Key Update Schemes 96
 - 7.3.1 Periodic Key Update 96
 - 7.3.2 Dynamic Key Update 99
 - 7.3.3 Session Keys and Key Reliability 102
 - 7.4 Reliability Analysis for Two-Factor Authentication Schemes . . . 103
 - 7.4.1 Electronic Token-Password Authentication Scheme 103
 - 7.4.2 Authentication with Two Dynamic Keys 106

- 8 Future Applications** 109
 - 8.1 Secure Mobile Transactions 109
 - 8.2 Software Identity by Patching History 111
 - 8.3 Energy Efficient Secure Wireless Communications 112

- Appendix A: Universal-2 Hash Functions** 115

- Appendix B: Shannon Entropy and Rényi Entropy** 117

- Appendix C: Proofs to Theorems in Section 6.5** 119

- Appendix D: Reliability Analysis for Dynamic Key Based Two-Factor Authentication** 123

- References** 127

- Index** 135