
COMPUTER SECURITY IN THE 21ST CENTURY

COMPUTER SECURITY IN THE 21ST CENTURY

Edited by
D. T. LEE
Academia Sinica, Taiwan

S. P. SHIEH
National Chiao Tung University, Taiwan

J. D. TYGAR
UC Berkeley

 Springer

Editors:

D.T. Lee
Academia Sinica, Taiwan

S.P. Shieh
National Chiao Tung University, Taiwan

J.D. Tygar
UC Berkeley

Computer Security in the 21st Century

Library of Congress Cataloging-in-Publication Data

Computer security in the 21st century / edited by D.T. Lee, S.P. Shieh, J.D. Tygar.
p. cm.

Includes bibliographical references and index.

ISBN 0-387-24005-5 (alk. paper) -- ISBN 0-387-24006-3 (e-ISBN)

I. Computer security. I. Title: Computer security in the twenty-first century. II. Lee, D. T. III. Shieh, S. P., 1960- IV. Tygar, J. D.

QA76.9A25C648 2005
005.8--dc22

2005042554

© 2005 Springer Science+Business Media, Inc.

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, Inc., 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 in the United States of America.

9 8 7 6 5 4 3 2 1

SPIN 11054160

springeronline.com

Contents

List of Figures	ix
1	
Introduction	1
<i>D. T. Lee, S. P. Shieh and J. D. Tygar</i>	
1. Acknowledgments	2
Part I Security Protocol Design	
2	
Challenges in Protocol Design and Analysis	7
<i>Dieter Gollmann</i>	
1. Introduction	7
2. Purpose of Analysis	8
3. The Environment	9
4. Case Studies	12
5. Conclusions and Challenges	21
References	22
3	
Private Matching	25
<i>Yaping Li, J. D. Tygar and Joseph M. Hellerstein</i>	
1. Introduction	25
2. Problem Statement	29
3. Threat Models	31
4. Terminology and Assumptions	33
5. Techniques	35
6. Data Ownership Certificate (DOC)	35
7. Security Analysis	41
8. Cost Analysis	47
9. Related Work	47
10. Future Work	48
References	49
4	
Authentication Protocol Analysis	51
<i>Jonathan Millen</i>	
1. Introduction	51

2.	Modeling Computational Operations	52
3.	Diffie-Hellman and Group Protocols	55
4.	Deeper Models of Encryption	56
5.	Decidable Formal Methods	56
6.	Future Directions	58
	References	58
5		
	Self-certified Approach for Authenticated Key Agreement	61
	<i>Tzong-Chen Wu and Yen-Ching Lin</i>	
1.	Introduction	61
2.	Proposed 2-PAKA Protocol	63
3.	Proposed n -PAKA Protocol	64
4.	Security Analysis	65
5.	Conclusion	66
	References	66
Part II P2P and Ad Hoc Networks		
6		
	Experimenting with Admission Control in P2P Networks	71
	<i>Nitesh Saxena, Gene Tsudik and Jeong Hyun Yi</i>	
1.	Introduction	72
2.	Background	73
3.	Bouncer: Admission Control Toolkit	75
4.	Integration with Peer Group Systems	79
5.	Experiments	83
6.	Discussion	86
7.	Future Directions	87
	References	88
7		
	Adaptive Random Key Distribution Schemes for Wireless Sensor Networks	91
	<i>Shih-I Huang, Shihpyng Shieh and S.Y. Wu</i>	
1.	Introduction	92
2.	Adaptive Random Pre-distribution Scheme	94
3.	Uniquely Assigned One-Way Hash Function Scheme	96
4.	Evaluation	97
5.	Conclusion	102
	References	102
Part III Intrusion Detection, Defense, Measurement		
8		
	Measuring Relative Attack Surfaces	109
	<i>Michael Howard, Jon Pincus and Jeannette M. Wing</i>	
1.	Introduction	110
2.	Terminology and Model	113

<i>Contents</i>	vii
3. Dimensions of an Attack Surface	117
4. Security Bulletins	121
5. Analyzing Attack Surfaces	125
6. An Example Attack Surface Metric	126
7. Discussion of the RASQ Approach	133
8. Related Work	134
9. Future Work	134
References	136
9	
A Modeling of Intrusion Detection Systems with Identification Capability	139
<i>Pei-Te Chen, Benjamin Tseng and Chi-Sung Laih</i>	
1. Introduction	139
2. Traditional IDS model	141
3. A New model based on Identification (IDSIC)	142
4. Conclusion	144
References	144
10	
A Source-End Defense System against DDoS Attacks	147
<i>Fu-Yuan Lee, Shiuhyng Shieh, Jui-Ting Shieh and Sheng-Hsuan Wang</i>	
1. Introduction	148
2. Review of D-WARD	151
3. Proposed System	153
4. Performance Evaluation	161
5. Conclusion and Future Work	166
References	167
11	
BEAGLE: Tracking System Failures for Reproducing Security Faults	169
<i>Chang-Hsien Tsai, Shih-Hung Liu, Shuen-Wen Huang, Shih-Kun Huang and Deron Liang</i>	
1. Introduction	170
2. The Detection of Control State Corruption	171
3. The BEAGLE System Design and Implementation	174
4. Experiments and Assessment	175
5. Related Work	176
6. Conclusions	178
References	179
Part IV Multimedia Security	
12	
Web Application Security—Past, Present, and Future	183
<i>Yao-Wen Huang and D. T. Lee</i>	
1. Introduction	184
2. Common Web Application Vulnerabilities	185
3. Current Countermeasures	187
4. Concluding Remarks and Future Work	214

References	218
13	
Securing JPEG2000 Code-Streams	229
<i>Robert H. Deng, Yongdong Wu and Di Ma</i>	
1. Introduction	230
2. Overview of JPEG2000 Code-streams	232
3. Overview of The Schemes	238
4. The Authentication Scheme	240
5. The Access Control Schemes	245
6. Conclusion	250
References	251
14	
A Secret Information Hiding Scheme Based on Switching Tree Coding	255
<i>Chin-Chen Chang, Tzu-Chuen Lu and Yi-Long Liu</i>	
1. Introduction	255
2. Related Work	256
3. Experiments	260
4. Conclusions	262
References	262
Index	265

List of Figures

2.1	Binding updates in Mobile IPv6	16
2.2	The Canvas protocol	18
2.3	An “attack” on the Canvas protocol; dotted lines indicate unused links.	19
3.1	AgES protocol	34
3.2	Security goals satisfied by the protocols in the malicious model. (*): Note that for these examples, we do not have a strong protocol. However, we do have a collusion-free strong protocol which is strong in the absence of colluding attacks . $X^{(1)}$ denotes a protocol is unspoofable in the absence of colluding adversaries.	42
3.3	Security goals satisfied by the protocols in the semi-honest model. (*): Note that for these examples, we do not have a strong protocol. However, we do have a collusion-free strong protocol which is strong in the absence of colluding attacks . $X^{(1)}$ denotes a protocol is unspoofable in the absence of colluding adversaries.	43
3.4	Cost analysis	46
6.1	Admission Control	74
6.2	GAC System Architecture	75
6.3	Dynamic Threshold Update Procedure	77
6.4	Binding GMC to PKC	78
6.5	GAC Packet Structure	78
6.6	Secure Gnutella Protocol Flow	80
6.7	Spread GAC Message Encapsulation	83
6.8	Basic Operation Cost	84
6.9	Signature Size	85
6.10	Gnutella Experiments	85
6.11	Secure Spread Experiments	86

7.1	Unordered key pool and the Two-Dimension key pool with $t = 10, s = 10$.	95
7.2	A key selection example	96
7.3	Comparison of different configured Two-Dimension Key Pool Selecting Schemes and Eschenauer's scheme (key pool size is 100,000)	99
7.4	Comparison of Random-pairwise keys scheme and UAO scheme in memory requirement and maximum supported network size.	102
8.1	Relative Attack Surface Quotient of Different Versions of Windows [Howard, 2003]	111
8.2	Microsoft Security Bulletin MS02-005a: Cumulative Patch for Internet Explorer (I)	122
8.3	Microsoft Security Bulletin MS02-005a: Cumulative Patch for Internet Explorer (II)	123
8.4	Mapping RASQ Attack Vectors into Our Formalism	129
8.5	Howard's Relative Attack Surface Quotient Metric	131
9.1	The roles and relationships in TIDSs.	141
9.2	The roles and components in IDSIC.	143
10.1	An example of the deployment of D-WARD	152
10.2	Average O/I values	154
10.3	Classification of Traffic Flow	157
10.4	Constant SYNC attack.	162
10.5	Pulsing SYNC attack.	162
10.6	Increasing SYNC attack.	163
10.7	Gradual SYNC attack.	163
10.8	Constant bandwidth overloading attack.	164
10.9	Pulsing bandwidth overloading attack.	165
10.10	Increasing bandwidth overloading attack.	165
10.11	Gradual bandwidth overloading attack.	166
11.1	A program with buffer overflow.	171
11.2	Process of the function wrapper generation	173
11.3	The architecture of Beagle	174
11.4	Calibration of the notepad.exe stack trace	176
11.5	The stack backtrace of the RobotFTP Server 1.0 with overlong input	176
12.1	Example of an XSS vulnerability.	185
12.2	Compromised HTML output.	186
12.3	Example of a SQL injection vulnerability.	186
12.4	Example of a general script injection vulnerability.	187

12.5	A more severe script injection bug.	187
12.6	Web application vulnerabilities result from insecure information flow, as illustrated using XSS.	190
12.7	An example of our test pattern for XSS.	195
12.8	System architecture of WAVES.	198
12.9	A comparison among static verification tools.	206
12.10	Primitive lattice.	209
12.11	Type-aware lattice.	209
12.12	Example A.	209
12.13	Example B.	209
12.14	Example of a false positive resulting from a type cast.	209
12.15	WebSSARI system architecture.	212
13.1	$n_R = 3$ resolutions of an image.	234
13.2	Two images of different qualities.	234
13.3	Partitioning resolutions into precincts.	236
13.4	Packet generation process.	237
13.5	Structure of a JPEG2000 code-stream.	237
13.6	Arrangement of packets in a code-stream following progression order layer-resolution-component-precinct.	237
13.7	A third party publication model.	238
13.8	The access control system setup.	239
13.9	An example Merkle hash tree.	241
13.10	The Merkle tree for a code-stream.	242
13.11	Merkle tree for an example code-stream.	243
13.12	The optimized Merkle tree.	244
13.13	An example optimized Merkle tree.	245
13.14	An example Sandhu tree.	247
13.15	Rooted tree for key generation for access control.	248
13.16	An example rooted tree for a code-stream with $n_R = 3$, $n_L = 3$, and $n_P = 2$.	250
14.1	Three binary connection trees.	258
14.2	The search order of STC.	258
14.3	The experimental images.	261