

Kan Zhang Yuliang Zheng (Eds.)

Information Security

7th International Conference, ISC 2004
Palo Alto, CA, USA, September 27-29, 2004
Proceedings



Springer

Table of Contents

Key Management

Practical Authenticated Key Agreement Using Passwords	1
<i>Taekyoung Kwon</i>	
Further Analysis of Password Authenticated Key Exchange Protocol Based on RSA for Imbalanced Wireless Networks	13
<i>Muxiang Zhang</i>	
Storage-Efficient Stateless Group Key Revocation	25
<i>Pan Wang, Peng Ning, Douglas S. Reeves</i>	

Digital Signatures

Low-Level Ideal Signatures and General Integrity Idealization	39
<i>Michael Backes, Birgit Pfitzmann, Michael Waidner</i>	
Cryptanalysis of a Verifiably Committed Signature Scheme Based on GPS and RSA	52
<i>Julien Cathalo, Benoît Libert, Jean-Jacques Quisquater</i>	
How to Break and Repair a Universally Composable Signature Functionality	61
<i>Michael Backes, Dennis Hofheinz</i>	

New Algorithms

RSA Accumulator Based Broadcast Encryption	73
<i>Craig Gentry, Zulfikar Ramzan</i>	
Chameleon Hashing Without Key Exposure	87
<i>Xiaofeng Chen, Fangguo Zhang, Kwangjo Kim</i>	
Radix-r Non-Adjacent Form	99
<i>Tsuyoshi Takagi, Sung-Ming Yen, Bo-Ching Wu</i>	

Cryptanalysis

On Related-Key and Collision Attacks: The Case for the IBM 4758 Cryptoprocessor	111
<i>Raphael C.-W. Phan, Helena Handschuh</i>	
Security Analysis of Two Signcryption Schemes	123
<i>Guilin Wang, Robert H. Deng, DongJin Kwak, SangJae Moon</i>	

On The Security of Key Derivation Functions.....	134
<i>Carlisle Adams, Guenther Kramer, Serge Mister, Robert Zuccherato</i>	

Intrusion Detection

Evaluating the Impact of Intrusion Detection Deficiencies on the Cost-Effectiveness of Attack Recovery	146
<i>Hai Wang, Peng Liu, Lunqun Li</i>	

A Model for the Semantics of Attack Signatures in Misuse Detection Systems	158
<i>Michael Meier</i>	

Detection of Sniffers in an Ethernet Network	170
<i>Zouheir Trabelsi, Hamza Rahmani</i>	

Using Greedy Hamiltonian Call Paths to Detect Stack Smashing Attacks.....	183
<i>Mark Foster, Joseph N. Wilson, Shigang Chen</i>	

Securing DBMS: Characterizing and Detecting Query Floods	195
<i>Elisa Bertino, Teodoro Leggieri, Evimaria Terzi</i>	

Access Control

An XML-Based Approach to Document Flow Verification	207
<i>Elisa Bertino, Elena Ferrari, Giovanni Mella</i>	

Model-Checking Access Control Policies	219
<i>Dimitar P. Guelev, Mark Ryan, Pierre Yves Schobbens</i>	

A Distributed High Assurance Reference Monitor	231
<i>Ajay Chander, Drew Dean, John Mitchell</i>	

Using Mediated Identity-Based Cryptography to Support Role-Based Access Control	245
<i>D. Nali, C. Adams, A. Miri</i>	

Human Authentication

Towards Human Interactive Proofs in the Text-Domain (Using the Problem of Sense-Ambiguity for Security)	257
<i>Richard Bergmair, Stefan Katzenbeisser</i>	

Image Recognition CAPTCHAs.....	268
<i>Monica Chew, J.D. Tygar</i>	

Certificate Management

A Hierarchical Key-Insulated Signature Scheme in the CA Trust Model	280
<i>Zhengyi Le, Ouyang Yi, James Ford, Fillia Makedon</i>	
Certificate Recommendations to Improve the Robustness of Web of Trust	292
<i>Qinglin Jiang, Douglas S. Reeves, Peng Ning</i>	

Mobile and Ad Hoc Security

Universally Composable Secure Mobile Agent Computation	304
<i>Ke Xu, Stephen R. Tate</i>	
Re-thinking Security in IP Based Micro-Mobility	318
<i>Jukka Ylitalo, Jan Melén, Pekka Nikander, Vesa Torvinen</i>	
Shared-Key Signature and Its Application to Anonymous Authentication in Ad Hoc Group	330
<i>Qianhong Wu, Xiaofeng Chen, Changjie Wang, Yumin Wang</i>	

Web Security

Prevent Online Identity Theft – Using Network Smart Cards for Secure Online Transactions	342
<i>HongQian Karen Lu, Asad Ali</i>	
Provable Unlinkability Against Traffic Analysis Already After $\mathcal{O}(\log(n))$ Steps!	354
<i>Marcin Gomułkiewicz, Marek Klonowski, Mirosław Kutylowski</i>	
An Efficient Online Electronic Cash with Unlinkable Exact Payments	367
<i>Toru Nakanishi, Mitsuaki Shiota, Yuji Sugiyama</i>	

Digital Rights Management

Modifiable Digital Content Protection in P2P	379
<i>Heejae Park, Jong Kim</i>	
Survey on the Technological Aspects of Digital Rights Management	391
<i>William Ku, Chi-Hung Chi</i>	
Detecting Software Theft via Whole Program Path Birthmarks	404
<i>Ginger Myles, Christian Collberg</i>	

Software Security

Effective Security Requirements Analysis: HAZOP and Use Cases	416
<i>Thitima Srivatanakul, John A. Clark, Fiona Polack</i>	

The Obfuscation Executive 428
 Kelly Heffner, Christian Collberg

Author Index 441