

Table of Contents

Network Security I

| | |
|---|---|
| A Dynamic Mechanism for Recovering from Buffer Overflow Attacks | 1 |
| <i>Stelios Sidiroglou, Giannis Giovanidis, and Angelos D. Keromytis</i> | |

| | |
|--|----|
| SVision: A Network Host-Centered Anomaly Visualization Technique | 16 |
| <i>Iosif-Viorel Onut, Bin Zhu, and Ali A. Ghorbani</i> | |

Trust & Privacy

| | |
|---|----|
| Time-Based Release of Confidential Information in Hierarchical Settings . | 29 |
| <i>Deholo Nali, Carlisle Adams, and Ali Miri</i> | |

| | |
|---|----|
| “Trust Engineering:” From Requirements to System Design and Maintenance – A Working National Lottery System Experience | 44 |
| <i>Elisavet Konstantinou, Vasiliki Liagkou, Paul Spirakis, Yannis C. Stamatiou, and Moti Yung</i> | |

| | |
|--|----|
| A Privacy-Preserving Rental System | 59 |
| <i>Yanjiang Yang and Beng Chin Ooi</i> | |

Key Management & Protocols

| | |
|--|----|
| Constant Round Dynamic Group Key Agreement | 74 |
| <i>Ratna Dutta and Rana Barua</i> | |

| | |
|---|----|
| A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design | 89 |
| <i>Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal Roy</i> | |

| | |
|--|-----|
| ID-based Multi-party Authenticated Key Agreement Protocols from Multilinear Forms | 104 |
| <i>Hyung Mok Lee, Kyung Ju Ha, and Kyo Min Ku</i> | |

| | |
|---|-----|
| On the Notion of Statistical Security in Simulatability Definitions | 118 |
| <i>Dennis Hofheinz and Dominique Unruh</i> | |

Public Key Encryption & Signature

| | |
|---|-----|
| Certificateless Public Key Encryption Without Pairing | 134 |
| <i>Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo</i> | |

| | |
|---|-----|
| Tracing-by-Linking Group Signatures | 149 |
| <i>Victor K. Wei</i> | |

| | |
|--|-----|
| Chaum's Designated Confirmer Signature Revisited | 164 |
| <i>Jean Monnerat and Serge Vaudenay</i> | |

Network Security II

| | |
|---|-----|
| gore: Routing-Assisted Defense Against DDoS Attacks | 179 |
| <i>Stephen T. Chou, Angelos Stavrou, John Ioannidis, and Angelos D. Keromytis</i> | |

| | |
|--|-----|
| IPSec Support in NAT-PT Scenario for IPv6 Transition | 194 |
| <i>Souhwan Jung, Jaeduck Choi, Younghun Kim, and Sungi Kim</i> | |

Signcryption

| | |
|--|-----|
| Hybrid Signcryption Schemes with Outsider Security | 203 |
| <i>Alexander W. Dent</i> | |

| | |
|--|-----|
| Analysis and Improvement of a Signcryption Scheme with Key Privacy . . | 218 |
| <i>Guomin Yang, Duncan S. Wong, and Xiaotie Deng</i> | |

| | |
|---|-----|
| Efficient and Proactive Threshold Signcryption | 233 |
| <i>Changshe Ma, Kefei Chen, Dong Zheng, and Shengli Liu</i> | |

Crypto Algorithm & Analysis

| | |
|---|-----|
| Error Oracle Attacks on CBC Mode: Is There a Future for CBC Mode Encryption? | 244 |
| <i>Chris J. Mitchell</i> | |

| | |
|---|-----|
| Hardware Architecture and Cost Estimates for Breaking SHA-1 | 259 |
| <i>Akashi Sato</i> | |

| | |
|--|-----|
| On the Security of Tweakable Modes of Operation: TBC and TAE | 274 |
| <i>Peng Wang, Dengguo Feng, and Wenling Wu</i> | |

| | |
|---|-----|
| A Non-redundant and Efficient Architecture for Karatsuba-Ofman Algorithm | 288 |
| <i>Nam Su Chang, Chang Han Kim, Young-Ho Park, and Jongin Lim</i> | |

Cryptography

| | |
|---|-----|
| Compatible Ideal Visual Cryptography Schemes with Reversing | 300 |
| <i>Chi-Ming Hu and Wen-Guey Tzeng</i> | |

| | |
|---|-----|
| An Oblivious Transfer Protocol with Log-Squared Communication | 314 |
| <i>Helger Lipmaa</i> | |

Applications

| | |
|---|-----|
| Electronic Voting: Starting Over? | 329 |
| <i>Yvo Desmedt and Kaoru Kurosawa</i> | |
| Timed-Release Encryption with Pre-open Capability and Its Application to Certified E-mail System | 344 |
| <i>Yong Ho Hwang, Dae Hyun Yum, and Pil Joong Lee</i> | |
| Universally Composable Time-Stamping Schemes with Audit | 359 |
| <i>Ahto Buldas, Peeter Laud, Märt Saarepera, and Jan Willemson</i> | |
| A Multiplicative Homomorphic Sealed-Bid Auction Based on Goldwasser-Micali Encryption | 374 |
| <i>Kun Peng, Colin Boyd, and Ed Dawson</i> | |

Software Security

| | |
|--|-----|
| Building a Cryptovirus Using Microsoft's Cryptographic API | 389 |
| <i>Adam L. Young</i> | |
| On the Security of the WinRAR Encryption Method | 402 |
| <i>Gary S.-W. Yeo and Raphael C.-W. Phan</i> | |
| Towards Better Software Tamper Resistance..... | 417 |
| <i>Hongxia Jin, Ginger Myles, and Jeffery Lotspiech</i> | |

Authorization & Access Control

| | |
|--|-----|
| Device-Enabled Authorization in the Grey System | 431 |
| <i>Lujo Bauer, Scott Garriss, Jonathan M. McCune, Michael K. Reiter, Jason Rouse, and Peter Rutenbar</i> | |
| Evaluating Access Control Policies Through Model Checking | 446 |
| <i>Nan Zhang, Mark Ryan, and Dimitar P. Guelev</i> | |
| A Cryptographic Solution for General Access Control..... | 461 |
| <i>Yibing Kong, Jennifer Seberry, Janusz R. Getta, and Ping Yu</i> | |

Student Papers

| | |
|--|-----|
| Integrity Improvements to an RFID Privacy Protection Protocol for Anti-counterfeiting | 474 |
| <i>Xiaolan Zhang and Brian King</i> | |
| A Formal Definition for Trust in Distributed Systems..... | 482 |
| <i>Daoxi Xiu and Zhaoyu Liu</i> | |

XII Table of Contents

| | |
|---|-----|
| A Practical Voting Scheme with Receipts | 490 |
| <i>Marek Klonowski, Mirosław Kutylowski, Anna Lauks, and Filip Zagórski</i> | |
| New Constructive Approach to Covert Channel Modeling and Channel Capacity Estimation | 498 |
| <i>Zhenghong Wang and Ruby B. Lee</i> | |
| Efficient Modeling of Discrete Events for Anomaly Detection Using Hidden Markov Models | 506 |
| <i>German Florez-Larrahondo, Susan M. Bridges, and Rayford Vaughn</i> | |
| Author Index | 515 |

Information Security

8th International Conference, ISC 2005, Singapore,

September 20-23, 2005, Proceedings

Zhou, J.; Deng, R.H.; Bao, F. (Eds.)

2005, XII, 520 p., Softcover

ISBN: 978-3-540-29001-8