

# 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  
*Carlisle Adams, Guenther Kramer, Serge Mister, Robert Zuccherato*

## Intrusion Detection

Evaluating the Impact of Intrusion Detection Deficiencies  
on the Cost-Effectiveness of Attack Recovery . . . . . 146  
*Hai Wang, Peng Liu, Lunqun Li*

A Model for the Semantics of Attack Signatures  
in Misuse Detection Systems . . . . . 158  
*Michael Meier*

Detection of Sniffers in an Ethernet Network . . . . . 170  
*Zouheir Trabelsi, Hamza Rahmani*

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

Securing DBMS: Characterizing and Detecting Query Floods . . . . . 195  
*Elisa Bertino, Teodoro Leggieri, Evimaria Terzi*

## Access Control

An XML-Based Approach to Document Flow Verification . . . . . 207  
*Elisa Bertino, Elena Ferrari, Giovanni Mella*

Model-Checking Access Control Policies . . . . . 219  
*Dimitar P. Guelev, Mark Ryan, Pierre Yves Schobbens*

A Distributed High Assurance Reference Monitor . . . . . 231  
*Ajay Chander, Drew Dean, John Mitchell*

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

## Human Authentication

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

Image Recognition CAPTCHAs . . . . . 268  
*Monica Chew, J.D. Tygar*

## Certificate Management

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

## Mobile and Ad Hoc Security

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

## Web Security

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

## Digital Rights Management

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

## Software Security

- Effective Security Requirements Analysis: HAZOP and Use Cases ..... 416  
*Thitima Srivatanakul, John A. Clark, Fiona Polack*

XII Table of Contents

The Obfuscation Executive.....	428
<i>Kelly Heffner, Christian Collberg</i>	
<b>Author Index</b> .....	441