

Table of Contents

Network Security I

- A Dynamic Mechanism for Recovering from Buffer Overflow Attacks 1
Stelios Sidiroglou, Giannis Giovanidis, and Angelos D. Keromytis
- SVision: A Network Host-Centered Anomaly Visualization Technique 16
Iosif-Viorel Onut, Bin Zhu, and Ali A. Ghorbani

Trust & Privacy

- Time-Based Release of Confidential Information in Hierarchical Settings . 29
Deholo Nali, Carlisle Adams, and Ali Miri
- “Trust Engineering:” From Requirements to System Design and
Maintenance – A Working National Lottery System Experience 44
*Elisavet Konstantinou, Vasiliki Liagkou, Paul Spirakis,
Yannis C. Stamatiou, and Moti Yung*
- A Privacy-Preserving Rental System 59
Yanjiang Yang and Beng Chin Ooi

Key Management & Protocols

- Constant Round Dynamic Group Key Agreement 74
Ratna Dutta and Rana Barua
- A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging
Blocks in Combinatorial Design 89
Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal Roy
- ID-based Multi-party Authenticated Key Agreement Protocols from
Multilinear Forms 104
Hyung Mok Lee, Kyung Ju Ha, and Kyo Min Ku
- On the Notion of Statistical Security in Simulatability Definitions 118
Dennis Hofheinz and Dominique Unruh

Public Key Encryption & Signature

- Certificateless Public Key Encryption Without Pairing 134
Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo
- Tracing-by-Linking Group Signatures 149
Victor K. Wei

Chaum’s Designated Confirmer Signature Revisited 164
Jean Monnerat and Serge Vaudenay

Network Security II

gore: Routing-Assisted Defense Against DDoS Attacks 179
*Stephen T. Chou, Angelos Stavrou, John Ioannidis, and
 Angelos D. Keromytis*

IPSec Support in NAT-PT Scenario for IPv6 Transition 194
Souhwan Jung, Jaeduck Choi, Younghan Kim, and Sungi Kim

Signcryption

Hybrid Signcryption Schemes with Outsider Security 203
Alexander W. Dent

Analysis and Improvement of a Signcryption Scheme with Key Privacy . . 218
Guomin Yang, Duncan S. Wong, and Xiaotie Deng

Efficient and Proactive Threshold Signcryption 233
Changshe Ma, Kefei Chen, Dong Zheng, and Shengli Liu

Crypto Algorithm & Analysis

Error Oracle Attacks on CBC Mode: Is There a Future for CBC Mode
 Encryption? 244
Chris J. Mitchell

Hardware Architecture and Cost Estimates for Breaking SHA-1 259
Akashi Satoh

On the Security of Tweakable Modes of Operation: TBC and TAE 274
Peng Wang, Dengguo Feng, and Wenling Wu

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

Cryptography

Compatible Ideal Visual Cryptography Schemes with Reversing 300
Chi-Ming Hu and Wen-Guey Tzeng

An Oblivious Transfer Protocol with Log-Squared Communication 314
Helger Lipmaa

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