

Table of Contents

Network Security

Model Checking of Security Protocols with Pre-configuration	1
<i>Kyoil Kim, Jacob A. Abraham, Jayanta Bhadra</i>	
Remote Access VPN with Port Protection Function by Mobile Codes	16
<i>Yoshiaki Shiraishi, Youji Fukuta, Masakatu Morii</i>	
A Role of DEVS Simulation for Information Assurance	27
<i>Sung-Do Chi, Jong Sou Park, Jang-Se Lee</i>	

Mobile Security

Enhancing Grid Security Infrastructure to Support Mobile Computing Nodes	42
<i>Kwok-Yan Lam, Xi-Bin Zhao, Siu-Leung Chung, Ming Gu, Jia-Guang Sun</i>	
Reliable Cascaded Delegation Scheme for Mobile Agent Environments . . .	55
<i>Hyun-suk Lee, Hyeog Man Kwon, Young Ik Eom</i>	
Practical Solution for Location Privacy in Mobile IPv6	69
<i>SuGil Choi, Kwangjo Kim, ByeongGon Kim</i>	

Intrusion Detection

CTAR: Classification Based on Temporal Class-Association Rules for Intrusion Detection	84
<i>Jin Suk Kim, Hohn Gyu Lee, Sungbo Seo, Keun Ho Ryu</i>	
Viterbi Algorithm for Intrusion Type Identification in Anomaly Detection System	97
<i>Ja-Min Koo, Sung-Bae Cho</i>	
Towards a Global Security Architecture for Intrusion Detection and Reaction Management	111
<i>Renaud Bidou, Julien Bourgeois, Francois Spies</i>	

Internet Security

Intrusion-Tolerant System Design for Web Server Survivability	124
<i>Dae-Sik Choi, Eul Gyu Im, Cheol-Won Lee</i>	

PANA/IKEv2: An Internet Authentication Protocol for Heterogeneous Access	135
<i>Paulo S. Pagliusi, Chris J. Mitchell</i>	

An Automatic Security Evaluation System for IPv6 Network	150
<i>Jaehoon Nah, Hyeokchan Kwon, Sungwon Sohn, Cheehang Park, Chimoon Han</i>	

Secure Software, Hardware, and Systems I

A Location Privacy Protection Mechanism for Smart Space	162
<i>Yeongsu Cho, Sangrae Cho, Daeseon Choi, Seunghun Jin, Kyoil Chung, Cheehang Park</i>	

Secure System Architecture Based on Dynamic Resource Reallocation ...	174
<i>Byoung Joon Min, Sung Ki Kim, Joong Sup Choi</i>	

Fair Exchange with Guardian Angels	188
<i>Gildas Avoine, Serge Vaudenay</i>	

Secure Software, Hardware, and Systems II

Sign-Based Differential Power Analysis	203
<i>Roman Novak</i>	

Asymmetric Watermarking Scheme Using Permutation Braids	217
<i>Geun-Sil Song, Mi-Ae Kim, Won-Hyung Lee</i>	

Low-Power Design of a Functional Unit for Arithmetic in Finite Fields $GF(p)$ and $GF(2^m)$	227
<i>Johann Großschädl, Guy-Armand Kamendje</i>	

E-commerce Security

Efficient Implementation of Relative Bid Privacy in Sealed-Bid Auction	244
<i>Kun Peng, Colin Boyd, Ed Dawson, Kapalee Viswanathan</i>	

Multi-dimensional Hash Chain for Sealed-Bid Auction	257
<i>Navapot Prakobpol, Yongyuth Permpoontanalarp</i>	

An Improved Forward Integrity Protocol for Mobile Agents	272
<i>Ming Yao, Ernest Foo, Kun Peng, Ed Dawson</i>	

Digital Rights Management

Taming “Trusted Platforms” by Operating System Design	286
<i>Ahmad-Reza Sadeghi, Christian Stübke</i>	

A Software Fingerprinting Scheme for Java Using Classfiles Obfuscation	303
<i>Kazuhide Fukushima, Kouichi Sakurai</i>	
Reducing Storage at Receivers in SD and LSD Broadcast Encryption Schemes	317
<i>Tomoyuki Asano</i>	
Biometrics and Human Interfaces I	
3D Face Recognition under Pose Varying Environments	333
<i>Hwanjong Song, Ukil Yang, Kwanghoon Sohn</i>	
An Empirical Study of Multi-mode Biometric Systems Using Face and Fingerprint	348
<i>H. Kang, Y. Han, H. Kim, W. Choi, Y. Chung</i>	
Fingerprint-Based Authentication for USB Token Systems	355
<i>Daesung Moon, Youn Hee Gil, Dosung Ahn, Sung Bum Pan, Yongwha Chung, Chee Hang Park</i>	
Biometrics and Human Interfaces II	
Iris Recognition System Using Wavelet Packet and Support Vector Machines	365
<i>Byungjun Son, Gyundo Kee, Yungcheol Byun, Yillbyung Lee</i>	
Biometrics Identification and Verification Using Projection-Based Face Recognition System	380
<i>Hyeonjoon Moon, Jaihie Kim</i>	
Visualization of Dynamic Characteristics in Two-Dimensional Time Series Patterns: An Application to Online Signature Verification	395
<i>Suyoung Chi, Jaeyeon Lee, Jung Soh, Dohyung Kim, Weongeun Oh, Changhun Kim</i>	
Public Key Cryptography / Key Management	
E-MHT. An Efficient Protocol for Certificate Status Checking	410
<i>Jose L. Muñoz, Jordi Forné, Oscar Esparza, Miguel Soriano</i>	
A Comment on Group Independent Threshold Sharing	425
<i>Brian King</i>	
Automation-Considered Logic of Authentication and Key Distribution ...	442
<i>Taekyoung Kwon, Seongan Lim</i>	

Applied Cryptography

The MESH Block Ciphers 458
 Jorge Nakahara Jr, Vincent Rijmen, Bart Preneel, Joos Vandewalle

Fast Scalar Multiplication Method Using Change-of-Basis Matrix
to Prevent Power Analysis Attacks on Koblitz Curves 474
 Dong Jin Park, Sang Gyoo Sim, Pil Joong Lee

Constructing and Cryptanalysis of a 16×16 Binary Matrix
as a Diffusion Layer 489
 Bon Wook Koo, Hwan Seok Jang, Jung Hwan Song

Author Index 505

Information Security Applications

4th International Workshop, WISA 2003, Jeju Island,
Korea, August 25-27, 2003, Revised Papers

Chae, K.; Yung, M. (Eds.)

2004, XII, 512 p., Softcover

ISBN: 978-3-540-20827-3