

# Table of Contents

## Invited Papers

ForNet: A Distributed Forensics Network .....	1
<i>K. Shanmugasundaram, N. Memon, A. Savant, and H. Bronnimann</i>	
Usage Control: A Vision for Next Generation Access Control .....	17
<i>R. Sandhu and J. Park</i>	
Implementing a Calculus for Distributed Access Control in Higher Order Logic and HOL .....	32
<i>T. Kosiyaatrakul, S. Older, P. Humenn, and S.-K. Chin</i>	
Complexity Problems in the Analysis of Information Systems Security ....	47
<i>A. Slissenko</i>	
A Behavior-Based Approach to Securing Email Systems .....	57
<i>S.J. Stolfo, S. Hershkop, K. Wang, O. Nimeskern, and C.-W. Hu</i>	
Real-Time Intrusion Detection with Emphasis on Insider Attacks .....	82
<i>S. Upadhyaya</i>	

## Mathematical Models and Architectures for Computer Network Security

Relating Process Algebras and Multiset Rewriting for Immediate Decryption Protocols .....	86
<i>S. Bistarelli, I. Cervesato, G. Lenzini, and F. Martinelli</i>	
GRID Security Review .....	100
<i>L. Gymnopoulos, S. Dritsas, S. Gritzalis, and C. Lambrinoudakis</i>	
A Knowledge-Based Repository Model for Security Policies Management ..	112
<i>S. Kokolakis, C. Lambrinoudakis, and D. Gritzalis</i>	
Symbolic Partial Model Checking for Security Analysis .....	122
<i>F. Martinelli</i>	
Rule-Based Systems Security Model .....	135
<i>M. Smirnov</i>	
Logical Resolving for Security Evaluation .....	147
<i>P.D. Zegzhda, D.P. Zegzhda, and M.O. Kalinin</i>	

## **Intrusion Detection**

Enhanced Correlation in an Intrusion Detection Process .....	157
<i>S. Benferhat, F. Autrel, and F. Cuppens</i>	
Safeguarding SCADA Systems with Anomaly Detection .....	171
<i>J. Bigham, D. Gamez, and N. Lu</i>	
Experiments with Simulation of Attacks against Computer Networks .....	183
<i>I. Kotenko and E. Man'kov</i>	
Detecting Malicious Codes by the Presence of Their "Gene of Self-replication" .....	195
<i>V.A. Skormin, D.H. Summerville, and J.S. Moronski</i>	
Automatic Generation of Finite State Automata for Detecting Intrusions Using System Call Sequences .....	206
<i>K. Wee and B. Moon</i>	

## **Public Key Distribution, Authentication, Access Control**

Distributed Access Control: A Logic-Based Approach .....	217
<i>S. Barker</i>	
Advanced Certificate Status Protocol .....	229
<i>D.H. Yum, J.E. Kang, and P.J. Lee</i>	
Key History Tree: Efficient Group Key Management with Off-Line Members .....	241
<i>A. Lain and V. Borisov</i>	
A Certificate Status Checking Protocol for the Authenticated Dictionary ..	255
<i>J.L. Munoz, J. Forne, O. Esparza, and M. Soriano</i>	
Context-Dependent Access Control for Web-Based Collaboration Environments with Role-Based Approach ...	267
<i>R. Wolf and M. Schneider</i>	

## **Cryptography**

A Signcryption Scheme Based on Secret Sharing Technique .....	279
<i>M. Al-Ibrahim</i>	
A Zero-Knowledge Identification Scheme Based on an Average-Case NP-Complete Problem .....	289
<i>P. Caballero-Gil and C. Hernández-Goya</i>	
Linear Cryptanalysis on SPECTR-H64 with Higher Order Differential Property .....	298
<i>Y.D. Ko, D.J. Hong, S.H. Hong, S.J. Lee, and J.L. Lim</i>	

Achievability of the Key-Capacity in a Scenario of Key Sharing by Public Discussion and in the Presence of Passive Eavesdropper . . . . .	308
<i>V. Korzhik, V. Yakovlev, and A. Sinuk</i>	
On Cipher Design Based on Switchable Controlled Operations . . . . .	316
<i>N.A. Moldovyan</i>	
Elliptic Curve Point Multiplication . . . . .	328
<i>A. Rostovtsev and E. Makhovenko</i>	
Encryption and Data Dependent Permutations: Implementation Cost and Performance Evaluation . . . . .	337
<i>N. Sklavos, A.A. Moldovyan, and O. Koufopavlou</i>	

## Steganography

Simulation-Based Exploration of SVD-Based Technique for Hidden Communication by Image Steganography Channel . . . . .	349
<i>V. Gorodetsky and V. Samoilov</i>	
Detection and Removal of Hidden Data in Images Embedded with Quantization Index Modulation . . . . .	360
<i>K. Zhang, S. Wang, and X. Zhang</i>	
Digital Watermarking under a Filtering and Additive Noise Attack Condition . . . . .	371
<i>V. Korzhik, G. Morales-Luna, I. Marakova, and C. Patiño-Ruvalcaba</i>	
Data Hiding in Digital Audio by Frequency Domain Dithering . . . . .	383
<i>S. Wang, X. Zhang, and K. Zhang</i>	
Steganography with Least Histogram Abnormality . . . . .	395
<i>X. Zhang, S. Wang, and K. Zhang</i>	
Multi-bit Watermarking Scheme Based on Addition of Orthogonal Sequences . . . . .	407
<i>X. Zhang, S. Wang, and K. Zhang</i>	

## Short Papers

Authentication of Anycast Communication . . . . .	419
<i>M. Al-Ibrahim and A. Cerny</i>	
Two-Stage Orthogonal Network Incident Detection for the Adaptive Coordination with SMTP Proxy . . . . .	424
<i>R. Ando and Y. Takefuji</i>	
Construction of the Covert Channels . . . . .	428
<i>A. Grusho and E. Timonina</i>	

Privacy and Data Protection in Electronic Communications .....	432
<i>L. Mitrou and K. Moulinos</i>	
Multiplier for Public-Key Cryptosystem Based on Cellular Automata .....	436
<i>H.S. Kim and S.H. Hwang</i>	
A Game Theoretic Approach to Analysis and Design of Survivable and Secure Systems and Protocols .....	440
<i>S. Kumar and V. Marbukh</i>	
Alert Triage on the ROC .....	444
<i>F.J. Martin and E. Plaza</i>	
Fast Ciphers for Cheap Hardware: Differential Analysis of SPECTR-H64 ..	449
<i>N.D. Goots, B.V. Izotov, A.A. Moldovyan, and N.A. Moldovyan</i>	
Immunocomputing Model of Intrusion Detection .....	453
<i>Y. Melnikov and A. Tarakanov</i>	
Agent Platform Security Architecture .....	457
<i>G. Santana, L.B. Sheremetov, and M. Contreras</i>	
Support Vector Machine Based ICMP Covert Channel Attack Detection ..	461
<i>T. Sohn, T. Noh, and J. Moon</i>	
Computer Immunology System with Variable Configuration .....	465
<i>S.P. Sokolova and R.S. Ivlev</i>	
<b>Author Index .....</b>	<b>469</b>

Computer Network Security

Second International Workshop on Mathematical  
Methods, Models, and Architectures for Computer  
Network Security, MMM-ACNS 2003, St. Petersburg,  
Russia, September 21-23, 2003, Proceedings  
Gorodetsky, V.; Popyack, L.; Skormin, V. (Eds.)  
2003, XIV, 478 p., Softcover  
ISBN: 978-3-540-40797-3