

Table of Contents

Invited Talks

An Intelligent Decision Support System for Intrusion Detection and Response	1
<i>Dipankar Dasgupta, Fabio A. Gonzalez</i>	
Mathematical Models of the Covert Channels	15
<i>Alexander Grusho</i>	
Open Issues in Formal Methods for Cryptographic Protocol Analysis	21
<i>Catherine Meadows</i>	
Future Directions in Role-Based Access Control Models	22
<i>Ravi Sandhu</i>	
Secure Networked Computing	27
<i>Vijay Varadharajan</i>	

Network Security Systems: Foundations, Models, and Architectures

Composability of Secrecy	28
<i>Jan Jürjens</i>	
Agent-Based Model of Computer Network Security System: A Case Study	39
<i>Vladimir I. Gorodetski, O. Karsayev, A. Khabalov, I. Kotenko, Leonard J. Popyack, Victor A. Skormin</i>	
Security Considerations and Models for Service Creation in Premium IP Networks	51
<i>Michael Smirnov</i>	
Secure Systems Design Technology	63
<i>Peter D. Zegzhda, Dmitry P. Zegzhda</i>	
A Privacy-Enhancing e-Business Model Based on Infomediaries	72
<i>Dimitris Gritzalis, Konstantinos Moulinos, Konstantinos Kostis</i>	
Applying <i>Practical</i> Formal Methods to the Specification and Analysis of Security Properties	84
<i>Constance Heitmeyer</i>	
Modeling Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ)	90
<i>Andrey Kostogryzov</i>	
Analyzing Separation of Duties in Petri Net Workflows	102
<i>Konstantin Knorr, Harald Weidner</i>	

Intrusion Detection: Foundations and Models

Information Security with Formal Immune Networks	115
<i>Alexander O. Tarakanov</i>	
BASIS: A Biological Approach to System Information Security	127
<i>Victor A. Skormin, Jose G. Delgado-Frias, Dennis L. McGee,</i> <i>Joseph V. Giordano, Leonard J. Popyack, Vladimir I. Gorodetski,</i> <i>Alexander O. Tarakanov</i>	
Learning Temporal Regularities of User Behavior for Anomaly Detection	143
<i>Alexandr Seleznyov, Oleksiy Mazhelis, Seppo Puuronen</i>	
Investigating and Evaluating Behavioural Profiling and Intrusion Detection Using Data Mining	153
<i>Harjit Singh, Steven Furnell, Benn Lines, Paul Dowland</i>	

Access Control, Authentication, and Authorization

Typed MSR: Syntax and Examples	159
<i>Iliano Cervesato</i>	
TRBAC ^N : A Temporal Authorization Model	178
<i>Steve Barker</i>	
The Set and Function Approach to Modeling Authorization in Distributed Systems	189
<i>Tatyana Ryutov, Clifford Neuman</i>	
Fenix Secure Operating System: Principles, Models, and Architecture ...	207
<i>Dmitry P. Zegzhda, Pavel G. Stepanov, Alexey D. Otavin</i>	

Cryptography and Steganography: Mathematical Basis, Protocols, and Applied Methods

Generalized Oblivious Transfer Protocols Based on Noisy Channels	219
<i>Valeri Korjik, Kirill Morozov</i>	
Controlled Operations as a Cryptographic Primitive	230
<i>Boris V. Izotov, Alexander A. Moldovyan, Nick A. Moldovyan</i>	
Key Distribution Protocol Based on Noisy Channel and Error Detecting Codes	242
<i>Viktor Yakovlev, Valery Korjik, Alexander Sinuk</i>	
Dynamic Group Key Management Protocol	251
<i>Ghassan Chaddoud, Isabelle Chrisment, André Schaff</i>	
SVD-Based Approach to Transparent Embedding Data into Digital Images	263
<i>Vladimir I. Gorodetski, Leonard J. Popyack, Vladimir Samoilov,</i> <i>Victor A. Skormin</i>	
Fast Encryption Algorithm Spectr-H64	275
<i>Nick D. Goots, Alexander A. Moldovyan, Nick A. Moldovyan</i>	

CVS at Work: A Report on New Failures upon Some Cryptographic Protocols	287
<i>Antonio Durante, Riccardo Focardi, Roberto Gorrieri</i>	
On Some Cryptographic Properties of Rijndael	300
<i>Selçuk Kavut, Melek D. Yücel</i>	
Author Index	313

<http://www.springer.com/978-3-540-42103-0>

Information Assurance in Computer Networks: Methods,
Models and Architectures for Network Security
International Workshop MMM-ACNS 2001 St.
Petersburg, Russia, May 21-23, 2001 Proceedings
Gorodetski, V.I.; Skormin, V.A.; Popyack, L.J. (Eds.)
2001, XIII, 316 p., Softcover
ISBN: 978-3-540-42103-0