Vladimir I. Gorodetski  Victor A. Skormin
Leonard J. Popyack (Eds.)

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
Preface

This volume contains the papers selected for presentation at the International Workshop on Mathematical Methods, Models and Architectures for Network Security Systems (MMM-ACNS 2001) held in St. Petersburg, Russia, May 21–23, 2001. The workshop was organized by the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) in cooperation with the Russian Foundation for Basic Research (RFBR), the US Air Force Research Laboratory (both the Information Directorate (AFRL/IF)) and the Office of Scientific Research (AFRL/OSR), and Binghamton University (USA).

MMM-ACNS 2001 provided an international forum for sharing original research results and application experiences among specialists in fundamental and applied problems of computer network security. An important distinction of the workshop was its focus on mathematical aspects of information and computer network security and the role of mathematical issues in contemporary and future development of models of secure computing.

A total of 36 papers coming from 12 different countries on significant aspects of both theory and applications of computer network and information security were submitted to MMM-ACNS 2001. Out of them 24 were selected for regular presentation. Five technical sessions were organized, namely: mathematical models for computer networks and applied systems security; methods and models for intrusion detection; mathematical basis and applied techniques of cryptography and steganography; applied techniques of cryptography; and models for access control, authentication, and authorization. Two panel discussions were devoted to the significant issues in the computer and information security field. The first sought to define the important open problems in computer security and to reach a conclusion as to mathematical methods and models can contribute, and the second focused upon security research and education in academia. The MMM-ACNS 2001 program was enriched by five invited speakers: Dipankar Dasgupta, Alexander Grusho, Catherine Meadows, Ravi Sandhu, and Vijay Varadharajan.

An event like this can only succeed as a result of team efforts. We would like to acknowledge the contribution of the Program Committee members and thank the reviewers for their efforts. Our sincere gratitude goes to all of the authors who submitted papers.

We are grateful to our sponsors: the European Office of Aerospace Research and Development (EOARD), the European Office of Naval Research International Field Office (ONRIFO), and the Russian Foundation of Basic Research (RFBR) for their generous support.

We wish to express our thanks to Alfred Hofmann of Springer-Verlag for his help and cooperation.

May 2001

Vladimir Gorodetski
Leonard Popyack
Victor Skormin
MMM-ACNS 2001 Workshop Committee

General Chairmen:

Victor Skormin          Watson School of Eng., Binghamton Univ., USA
Rafael Yusupov          St. Petersburg Inst. for Informatics and Automation, Russia

International Organizing Committee

Barry Mckiney           Air Force Research Laboratory/IF, USA
Michael Morgan           Office of Naval Research Int. Field Office, USA
Christopher Reuter       European Office of Aerospace R&D, USA
Rafael Yusupov           St. Petersburg Inst. for Informatics and Automation, Russia
Program Committee

Program Co-chairmen:

Vladimir Gorodetski  St. Petersburg Inst. for Informatics and Automation, Russia
Leonard Popyack  Air Force Research Laboratory/IF, USA
Victor Skormin  Watson School of Eng., Binghamton Univ., USA

International Program Committee

Kurt Bauknecht  Univ. of Zurich, Dept. of Information Technology, Switzerland
Harold Carter  University of Cincinnati, USA
Peter Chen  Computer Science Dept., Luisiana State Univ., USA
Dipankar Dasgupta  Div. of Computer Science, Univ. of Memphis, USA
Jose G. Delgado-Frias  Electrical and Comp. Eng. Dept., Univ. of Virginia, USA
Lynette Drevin  Comp. Science and Inf. Systems, Potchefstroom Univ., South Africa
Jiri Fridrich  Watson School of Eng., Binghamton Univ., USA
Dimitris Gritzalis  Athens Univ. of Economics & Business, Greece
Alexander Grusho  Russian State Univ. for Humanity, Russia
Yury Karpov  St. Petersburg State Technical Univ., Russia
Igor Kotenko  St. Petersburg Inst. for Informatics and Automation, Russia
Martin Kutter  AlpVision, Les Paccots, Switzerland
Anatoly Maliuk  Moscow State Engineering Physical Inst., Russia
Catherine Meadows  Naval Research Laboratory, USA
Nikolay Moldovian  Spec. Center of Program Systems “SPECTR”, Russia
Vladimir Orlov  Microtest Company, Moscow, Russia
Gyorgy Papp  V.R.A.M. Communication Ltd., Hungary
Hartmut Pohl  Fachhochschule Bonn-Rhein-Sieg, St. Augustin-Univ. of Applied Sciences, Germany
Ravi Sandhu  SingleSignOn.Net Inc. and George Mason Univ., USA
Igor Sokolov  Inst. for Informatics Problems, Moscow, Russia
Mikhail Sycheov  Bauman State Technical Univ., Russia
Leonid Ukhlinov  The State Customs Committee of Russia, Russia
Vijay Varadharajan  Div. of Inf. and Commun. Sciences Macquarie Univ., Australia
Minerva M. Yeung  Media and Internet Technology, Intel, USA
Louise Yngstrom  Dept. of Comp. and Systems Sciences, Univ. & Royal Inst. of Technology, Stockholm
Peter Zegzhda  St. Petersburg State Technical Univ., Russia
Reviewers

Kurt Bauknecht  Univ. of Zurich, Dept. of Information Technology, Switzerland
Kirill Bolshakov  St. Petersburg State Technical Univ., Russia
Dipankar Dasgupta  Div. of Comp. Science, Univ. of Memphis, USA
Gunther Drevin  Comp. Science and Inf. Systems, Potchefstroom Univ., South Africa
Lynette Drevin  Comp. Science and Inf. Systems, Potchefstroom Univ., South Africa
Dimitris Gritzalis  Athens Univ. of Economics & Business, Greece
Vladimir Gorodetski  St. Petersburg Inst. for Informatics and Automation, Russia
Yury Karpov  St. Petersburg State Technical Univ., Russia
Igor Kotenko  St. Petersburg Inst. for Informatics and Automation, Russia
Evgenii Krouk  St. Petersburg State Technical Univ., Russia
Catherine Meadows  Naval Research Laboratory, USA
Nikolay Moldovian  Spec. Center of Program Systems “SPECTR”, Russia
Gyorgy Papp  V.R.A.M. Communication Ltd., Hungary
Vladimir Platonov  St. Petersburg State Technical Univ., Russia
Alexander Rostovtsev  St. Petersburg State Technical Univ., Russia
Ravi Sandhu  SingleSignOn.Net Inc. and George Mason University, USA
Michael Smirnow  GMD, FOKUS, Germany
Igor Sokolov  Inst. for Informatics Problems, Moscow, Russia
Vijay Varadharajan  Div. of Inf. and Commun. Sciences, Macquarie Univ., Australia
Dmitry Zegzhda  St. Petersburg State Technical Univ., Russia
Peter Zegzhda  St. Petersburg State Technical Univ., Russia
# Table of Contents

**Invited Talks**

An Intelligent Decision Support System for Intrusion Detection and Response .................................................. 1  
*Dipankar Dasgupta, Fabio A. Gonzalez*

Mathematical Models of the Covert Channels ............................. 15  
*Alexander Grusho*

Open Issues in Formal Methods for Cryptographic Protocol Analysis  .... 21  
*Catherine Meadows*

Future Directions in Role-Based Access Control Models .................. 22  
*Ravi Sandhu*

Secure Networked Computing .................................................. 27  
*Vijay Varadharajan*

**Network Security Systems: Foundations, Models, and Architectures**

Composability of Secrecy ...................................................... 28  
*Jan Järjens*

Agent-Based Model of Computer Network Security System: A Case Study 39  

Security Considerations and Models for Service Creation in Premium IP Networks ........................................ 51  
*Michael Smirnov*

Secure Systems Design Technology ............................................. 63  
*Peter D. Zegzhda, Dmitry P. Zegzhda*

A Privacy-Enhancing e-Business Model Based on Infomediaries .......... 72  
*Dimitris Gritzalis, Konstantinos Moulinos, Konstantinos Kostis*

Applying Practical Formal Methods to the Specification and Analysis of Security Properties ................................. 84  
*Constance Heitmeyer*

Modeling Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ) ........................................ 90  
*Andrey Kostogryzov*

Analyzing Separation of Duties in Petri Net Workflows .................. 102  
*Konstantin Knorr, Harald Weidner*
Intrusion Detection: Foundations and Models

Information Security with Formal Immune Networks ....................... 115
Alexander O. Tarakanov

BASIS: A Biological Approach to System Information Security .......... 127
Victor A. Skormin, Jose G. Delgado-Frias, Dennis L. McGee,
Joseph V. Giordano, Leonard J. Popyack, Vladimir I. Gorodetski,
Alexander O. Tarakanov

Learning Temporal Regularities of User Behavior for Anomaly Detection 143
Alexandr Seleznyov, Oleksiy Mazhelis, Seppo Puuronen

Investigating and Evaluating Behavioural Profiling
and Intrusion Detection Using Data Mining ...................................... 153
Harjit Singh, Steven Furnell, Benn Lines, Paul Dowland

Access Control, Authentication, and Authorization

Typed MSR: Syntax and Examples .................................................. 159
Iliano Cervesato

TRBACN: A Temporal Authorization Model ...................................... 178
Steve Barker

The Set and Function Approach to Modeling Authorization
in Distributed Systems ................................................................. 189
Tatyana Ryutov, Clifford Neuman

Fenix Secure Operating System: Principles, Models, and Architecture . . 207
Dmitry P. Zegzhda, Pavel G. Stepanov, Alexey D. Otavin

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

Generalized Oblivious Transfer Protocols Based on Noisy Channels ...... 219
Valeri Korjik, Kirill Morozov

Controlled Operations as a Cryptographic Primitive ......................... 230
Boris V. Izotov, Alexander A. Moldovyan, Nick A. Moldovyan

Key Distribution Protocol Based on Noisy Channel
and Error Detecting Codes ......................................................... 242
Viktor Yakovlev, Valery Korjik, Alexander Sinuk

Dynamic Group Key Management Protocol ................................... 251
Ghassan Chaddoud, Isabelle Chrisment, André Schaff

SVD-Based Approach to Transparent Embedding Data
into Digital Images ................................................................. 263
Vladimir I. Gorodetski, Leonard J. Popyack, Vladimir Samoilov,
Victor A. Skormin

Fast Encryption Algorithm Spectr-H64 .......................................... 275
Nick D. Goots, Alexander A. Moldovyan, Nick A. Moldovyan
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVS at Work: A Report on New Failures upon Some Cryptographic Protocols</td>
<td>287</td>
</tr>
<tr>
<td>Antonio Durante, Riccardo Focardi, Roberto Gorrieri</td>
<td></td>
</tr>
<tr>
<td>On Some Cryptographic Properties of Rijndael</td>
<td>300</td>
</tr>
<tr>
<td>Selçuk Kavut, Melek D. Yücel</td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>313</td>
</tr>
</tbody>
</table>