Preface

This volume contains papers presented at the Fourth International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2007) held in St. Petersburg, Russia, during September 13–15, 2007. The workshop was organized by the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) in cooperation with Binghamton University (SUNY, USA).

The organizers are proud that the MMM-ACNS workshops hosted by the St. Petersburg Institute for Informatics and Automation in 2001, 2003 and 2005 evolved into a bi-annual series recognized in the professional community. These events not only demonstrated the keen interest of the participating researchers in the subject matter and the opportunity to present and disseminate individual achievements, but also promoted the spirit of cooperation, camaraderie, free exchange of ideas, and intellectually stimulating interaction between colleagues.

Again, MMM-ACNS 2007 provided an international forum for sharing original research results among specialists in fundamental and applied problems of computer network security. An important distinction of the conference was its focus on mathematical aspects of information and computer network security addressing the ever-increasing demands for secure computing and highly dependable computer networks.

A total of 56 papers from 18 countries related to significant aspects of both theory and applications of computer network and information security were submitted to MMM-ACNS 2007. In total, 18 papers were selected for regular presentations and 12 for short presentations (32 % of acceptance for full papers and 53 % for all papers).

The MMM-ACNS 2007 program was enriched by invited papers presented by six distinguished invited speakers: Christian Collberg (University of Arizona, USA), Angelos D. Keromytis (Columbia University, USA), Paulo Verissimo (University of Lisbon, Portugal), Jean-Daniel Aussel (Gemalto, France), Mauricio Sanchez (ProCurve Networking, HP, USA) and Victor Serdiouk (DialogueScience, Inc., Russia) addressing important theoretical aspects and advanced applications.

The success of the workshop was assured by the team efforts of sponsors, organizers, reviewers and participants. We would like to acknowledge the contributions of the individual Program Committee members and thank the paper reviewers.

Our sincere gratitude goes to the participants of the workshop and all authors of the submitted papers. We are grateful to our sponsors: European Office of Aerospace Research and Development (EOARD) of the U.S. Air Force and the U.S. Office of Naval Research Global (ONRGlobal) for their generous support.
We also wish to express our gratitude to the Springer LNCS team managed by Alfred Hofmann for their help and cooperation.

September 2007

Vladimir Gorodetsky
Igor Kotenko
Victor Skormin
Organization

Workshop Chairmen

General Chairs
Rafael M. Yusupov  St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Russia
Robert L. Herklotz  US Air Force Office of Scientific Research, USA

Program Committee Co-chairs
Vladimir Gorodetsky  St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Russia
Igor Kotenko  St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Russia
Victor Skormin  Binghamton University, State University of New York; National Research Council’s Senior Research Associate with the Air Force, USA

Program Committee
Julien Bourgeois  University of Franche-Comte, France
David Chadwick  University of Kent, UK
Shiu-Kai Chin  Syracuse University, USA
Howard Chivers  Cranfield University, UK
Christian Collberg  University of Arizona, USA
Dipankar Dasgupta  University of Memphis, USA
Naranker Dulay  Imperial College London, UK
Dieter Gollmann  Hamburg University of Technology, Germany
Dimitris Gritzalis  Athens University of Economics and Business, Greece
Stefanos Gritzalis  University of the Aegean, Greece
Alexander Grusho  Moscow State University, Russia
Ming-Yuh Huang  The Boeing Company, USA
Sushil Jajodia  George Mason University, USA
Angelos Keromytis  Columbia University, USA
Victor Korneev  Federal Enterprise “R&D Institute “Kvant”, Russia
Klaus-Peter Kossakowski  Presecure Consulting GmbH, Germany
Christopher Kruegel  Technical University of Vienna, Austria
Antonio Lioy  Politecnico di Torino, Italy
Javier Lopez  University of Malaga, Spain
Fabio Martinelli  CNR/IIT, Italy
Catherine Meadows  Naval Research Laboratory, USA
Nasir Memon  Polytechnic University Brooklyn, USA
Ann Miller  University of Missouri - Rolla, USA
Nikolay Moldovyan  Specialized Center of Program Systems “SPECTR”, Russia
Wojciech Molisz  Gdansk University of Technology, Poland
David Nicol  University of Illinois at Urbana-Champaign, USA
Yoram Ofek  University of Trento, Italy
Monika Oit  Cybernetica, Estonia
Udo Prayer  IAIK, Austria
Bart Preneel  Katholieke Universiteit Leuven, Belgium
Roland Rieke  Fraunhofer Institute for Secure Information Technology SIT, Germany
Andrei Sabelfeld  Chalmers University of Technology, Sweden
Ravi Sandhu  George Mason University and NSD Security, USA
Antonio Gomez Skarmeta  University of Murcia, Spain
Anatol Slissenko  University Paris-12, France
Michael Smirnov  Fraunhofer-Gesellschaft Institute FOKUS, Germany
Igor Sokolov  The Institute of Informatics Problems of the Russian Academy of Sciences, Russia
Douglas Summerville  Binghamton University, USA
Shambhu Upadhyaya  University at Buffalo, USA
Alfonso Valdes  SRI International, USA
Vijay Varadharajaran  Macquarie University, Australia
Valery Vasenin  Moscow State University, Russia
Paulo Verissimo  University of Lisbon, Portugal
Diego Zamboni  IBM, Switzerland
Peter Zegzhda  St. Petersburg Polytechnical University, Russia

Reviewers

Elli Androulaki  Columbia University, USA
Daniele Beauquier  University Paris-12, France
Julien Bourgeois  University of Franche-Comte, France
David Chadwick  University of Kent, UK
Nikolaos Chatzis  Fraunhofer-Gesellschaft Institute FOKUS, Germany
Shiu-Kai Chin  Syracuse University, USA
Howard Chivers  Cranfield University, UK
Christian Collberg  University of Arizona, USA
Table of Contents

Invited Papers

Academia Track

Surreptitious Software: Models from Biology and History
Christian Collberg, Jasvir Nagra, and Fei-Yue Wang

Characterizing Software Self-healing Systems
Angelos D. Keromytis

Assumptions: The Trojan Horses of Secure Protocols
Paulo Verissimo

Industry Track

Smart Cards and Digital Security
Jean-Daniel Aussel

Virus Throttle as Basis for ProActive Defense
Mauricio Sanchez

Technologies for Protection Against Insider Attacks on Computer Systems
Victor Serdiouk

Authentication, Authorization and Access Control

Full Papers

Access Control and Declassification
Gérard Boudol and Marija Kolundžija

Reasoning About Delegation and Account Access in Retail Payment Systems
Shiu-Kai Chin and Susan Older

Performance Evaluation of Keyless Authentication Based on Noisy Channel
Valery Korzhik, Viktor Yakovlev, Guillermo Morales-Luna, and Roman Chesnokov

Avoiding Key Redistribution in Key Assignment Schemes
Harry Rowe and Jason Crampton
## Short Papers

**Fern : An Updatable Authenticated Dictionary Suitable for Distributed Caching**  
E. Freudenthal, D. Herrera, S. Gutstein, R. Spring, and L. Longpré  
141

**Class of Provably Secure Information Authentication Systems**  
N.A. Moldovyan and A.A. Moldovyan  
147

**A New Modeling Paradigm for Dynamic Authorization in Multi-domain Systems**  
Manoj Sastry, Ram Krishnan, and Ravi Sandhu  
153

## Language-Based Security, Trust Management and Covert Channels

## Full Papers

**Synthesis of Non-interferent Distributed Systems**  
Franck Cassez, John Mullins, and Olivier H. Roux  
159

**Privacy-Preserving Credential Verification for Non-monotonic Trust Management Systems**  
Changyu Dong, Giovanni Russello, and Naranker Dulay  
171

**Covert Channel Invisibility Theorem**  
Alexander Grusho, Nick Grebnev, and Elena Timonina  
187

## Security Verification and Evaluation

## Full Papers

**Policy-Based Proactive Monitoring of Security Policy Performance**  
Vitaly Bogdanov and Igor Kotenko  
197

**Comparing Electronic Battlefields: Using Mean Time-To-Compromise as a Comparative Security Metric**  
David John Leversage and Eric James Byres  
213

**Abstraction Based Verification of a Parameterised Policy Controlled System**  
Peter Ochsenschläger and Roland Rieke  
228

## Short Papers

**Algebraic Models to Detect and Solve Policy Conflicts**  
Cataldo Basile, Alberto Cappadonia, and Antonio Lioy  
242
### Intrusion Detection and Prevention

#### Full Papers

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-agent Peer-to-Peer Intrusion Detection</td>
<td>260</td>
</tr>
<tr>
<td>Vladimir Gorodetsky, Oleg Karsaev, Vladimir Samoylov, and Sergey Serebryakov</td>
<td></td>
</tr>
<tr>
<td>An Interval Temporal Logic-Based Matching Framework for Finding Occurrences of Multi-event Attack Signatures</td>
<td>272</td>
</tr>
<tr>
<td>Elżbieta Nowicka and Marcin Zawada</td>
<td></td>
</tr>
<tr>
<td>Towards Fully Automatic Defense Mechanism for a Computer Network</td>
<td>286</td>
</tr>
<tr>
<td>V. Skormin, O. Shiryayeva, A. Tokhtabayev, and J. Moronski</td>
<td></td>
</tr>
<tr>
<td>Mathematical Models of Intrusion Detection by an Intelligent Immunochip</td>
<td>308</td>
</tr>
<tr>
<td>Alexander O. Tarakanov</td>
<td></td>
</tr>
<tr>
<td>A Novel Intrusion Detection System for a Local Computer Network</td>
<td>320</td>
</tr>
<tr>
<td>A. Tokhtabayev, A. Altaibek, V. Skormin, and U. Tukeyev</td>
<td></td>
</tr>
</tbody>
</table>

#### Short Papers

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation of the Effectiveness of Alert Correlation Methods in a Policy-Based Security Framework</td>
<td>334</td>
</tr>
<tr>
<td>Bartłomiej Balcerek, Piotr Dragan, Bogdan Trawiński, and Marcin Wajtkiewicz</td>
<td></td>
</tr>
<tr>
<td>Host-Based Intrusion Detection System: Model and Design Features</td>
<td>340</td>
</tr>
<tr>
<td>Pyotr Zegzhda and Semyon Kort</td>
<td></td>
</tr>
</tbody>
</table>

### Network Survivability and Privacy

#### Full Papers

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval Approach to Preserving Privacy in Statistical Databases: Related Challenges and Algorithms of Computational Statistics</td>
<td>346</td>
</tr>
<tr>
<td>Luc Longpré, Gang Xiang, Vladik Kreinovich, and Eric Freudenthal</td>
<td></td>
</tr>
</tbody>
</table>
Fast Service Restoration Under Shared Protection at Lightpath Level in Survivable WDM Mesh Grooming Networks 362
   Jacek Rak and Wojciech Molisz

Anycast Communication – A New Approach to Survivability of Connection-Oriented Networks 378
   Krzysztof Walkowiak

**Short Papers**

Privacy Preserving Context Transfer in All-IP Networks 390
   Giorgos Karopoulos, Georgios Kambourakis, and Stefanos Gritzalis

Environment-Aware Trusted Data Delivery in Multipath Wireless Protocols 396
   Mohit Virendra, Arunn Krishnamurthy, Krishnan Narayanan, Shambhu Upadhyaya, and Kevin Kwiat

**Watermarking**

**Short Papers**

A Spatial Watermarking Algorithm for Video Images 402
   Dumitru Dan Burdescu, Liana Stanescu, Anca Ion, and Cristian Marian Mihaescu

Watermarking Software to Signal Copy Protection 408
   Ernő Jeges, Zoltán Hornák, Gergely Eberhardt, and Zoltán Nagy

**Author Index** 415