Lecture Notes in Computer Science 2776

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Vladimir Gorodetsky Leonard Popyack
Victor Skormin (Eds.)

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

Springer

Volume Editors

Vladimir Gorodetsky
St. Petersburg Institute for Informatics and Automation
Intelligent Systems Laboratory
39, 14-th Liniya, St. Petersburg, 199178, Russia
E-mail: gor@mail.iias.spb.su

Leonard Popyack
Syracuse University
Syracuse, NY 13244, USA
E-mail: popyack@rl.af.mil

Victor Skormin
Binghamton University, Watson School of Engineering
Binghamton, NY 13902, USA
E-mail: vskormin@binghamton.edu

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): C.2, D.4.6, E.3, K.6.5, K.4.1, K.4.4, J.1

ISSN 0302-9743
ISBN 3-540-40797-9 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 10931417 06/3142 5 4 3 2 1 0

Preface

This volume contains the papers presented at the International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2003) held in St. Petersburg, Russia, during September 21–23, 2003. 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/Information Directorate (AFRL/IF) and the Air Force Office of Scientific Research (AFOSR), the Office of Naval Research International Field Office (USA), and Binghamton University (SUNY, USA).

The first international workshop of this series, MMM-ACNS 2001, May 21–23, 2001, St. Petersburg, Russia, hosted by the St. Petersburg Institute for Informatics and Automation, demonstrated the keen interest of the international research community in the theoretical aspects of computer network and information security and encouraged the establishment of an on-going series of brennial workshops.

MMM-ACNS 2003 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 62 papers from 18 countries related to significant aspects of both the theory and the applications of computer-network and information security were submitted to MMM-ACNS 2003. Out of them 29 were selected for regular and 12 for short presentations. Five technical sessions were organized, namely: mathematical models for computer network security; methods, models, and systems for intrusion detection; methods and models for public key infrastructure, access control and authentication; mathematical basis and applied techniques of cryptography; and steganographic algorithms. The panel discussion was devoted to the challenging problems in intrusion detection. The MMM-ACNS 2003 program was enriched by six distinguished invited speakers: Dr. Shiu-Kai Chin, Dr. Nasir Memon, Dr. Ravi Sandhu, Dr. Anatol Slissenko, Dr. Salvatore Stolfo, and Dr. Shambhu Upadhyaya.

The success of the workshop was assured by team efforts of sponsors, organizers, reviewers, and participants. We would like to acknowledge the contribution of the individual program committee members and thank the paper reviewers. Our sincere gratitude goes to the participants of the workshop and all the authors of the 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), the Russian Foundation for Basic Research

(RFBR), and the Ministry of Industry, Technical Policy, and Science of the Russian Federation for their generous support.

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

September 2003

Vladimir Gorodetsky
Leonard Popyack
Victor Skormin

MMM-ACNS 2003 Workshop Committee

General Chairmen:

Rafael M. Yusupov	St. Petersburg Institute for Informatics and Automation, Russia
Robert L. Herklotz	Air Force Office of Scientific Research, USA

Program Committee Co-chairmen:

Vladimir Gorodetsky	St. Petersburg Institute for Informatics and Automation, Russia
Leonard Popyack	Air Force Research Laboratory/IF, USA
Victor Skormin	Watson School of Engineering, Binghamton University, USA

International Program Committee

Kurt Bauknecht	University of Zurich, Department of Information Technology, Switzerland
John Bigham	Department of Electronic Engineering, Queen Mary, University of London, UK
Wes Carter	Department of Electronic Engineering, Queen Mary, University of London, UK
Riccardo Focardi	University of Venice, Italy
Dipankar Dasgupta	University of Memphis, USA
Alexey Galatenko	Moscow State University, Russia
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Alexander Grusho	Russian State University for Humanity, Russia
Yuri Karpov	St. Petersburg Polytechnical University, Russia
Valery Korzhik	Specialized Center of Program Systems "SPECTR", Russia
Igor Kotenko	St. Petersburg Institute for Informatics and Automation, Russia
Catherine Meadows	Naval Research Laboratory, USA
Bret Michael	Naval Postgraduate School, USA
Ann Miller	University of Missouri – Rolla, USA
Nikolay Moldovyan	Specialized Center of Program Systems "SPECTR", Russia
Ravi Sandhu	George Mason University and NSD Security, USA
Michael Smirnov	Fraunhofer-Gesellschaft Institute FOKUS, Germany
Igor Sokolov	Institute for Informatics Problems, Russia
Salvatore J. Stolfo	Department of Computer Science, Columbia University, USA
Douglas H. Summerville	Binghamton University, USA
Alfonso Valdes	SRI International, USA
Vijay Varadharajaran	Macquarie University, Australia
Nikoly Zagoruiko	Sobolev Institute of Mathematics, Siberian Branch of RAS, Russia
Peter Zegzhda	St. Petersburg Polytechnical University, Russia

Reviewers

Kurt Bauknecht	University of Zurich, Department of Information Technology, Switzerland
John Bigham	Department of Electronic Engineering, Queen Mary, University of London, UK
David Bonyuet	Delta Search Labs, USA
Wes Carter	Department of Electronic Engineering, Queen Mary, University of London, UK
Sergei Fedorenko	St. Petersburg Polytechnical University, Russia
Riccardo Focardi	University of Venice, Italy
Jessica Fridrich	Binghamton University, USA
Dipankar Dasgupta	University of Memphis, USA
Vladimir Gorodetsky	St. Petersburg Institute for Informatics and Automation, Russia
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Alexander Grusho	Russian State University for Humanity, Russia
Boris Izotov	Specialized Center of Program Systems "SPECTR", Russia
Maxim Kalinin	St. Petersburg Polytechnical University, Russia
Yuri Karpov	St. Petersburg Polytechnical University, Russia
Valery Korzhik (Russia)	Specialized Center of Program Systems "SPECTR"
Igor Kotenko	St. Petersburg Institute for Informatics and Automation, Russia
Catherine Meadows	Naval Research Laboratory, USA
Bret Michael	Naval Postgraduate School, USA
Ann Miller	University of Missouri – Rolla, USA
Nikolay Moldovyan	Specialized Center of Program Systems "SPECTR", Russia
Alexander Rostovtsev	St. Petersburg Polytechnical University, Russia
Ravi Sandhu	George Mason University and NSD Security, USA
Nicolas Sklavos	Electrical and Computer Engineering Department, University of Patras, Greece
Victor Skormin	Watson School of Engineering, Binghamton University, USA
Anatol Slissenko	University Paris-12, France
Michael Smirnov	Fraunhofer-Gesellschaft Institute FOKUS, Germany
Igor Sokolov	Institute for Informatics Problems, Russia
Douglas H. Summerville	Binghamton University, SUNY, USA
Alfonso Valdes	SRI International, USA
Nikoly Zagoruiko	Sobolev Institute of Mathematics, Siberian Branch of RAS, Russia
Dmitry Zegzhda	St. Petersburg Polytechnical University, Russia

Table of Contents

Invited Papers

ForNet: A Distributed Forensics Network 1
K. Shanmugasundaram, N. Memon, A. Savant, and H. Bronnimann

Usage Control: A Vision for Next Generation Access Control 17
R. Sandhu and J. Park

Implementing a Calculus for Distributed Access Control in Higher Order Logic and HOL 32
T. Kosiyatrakul, S. Older, P. Humenn, and S.-K. Chin

Complexity Problems in the Analysis of Information Systems Security 47
A. Slissenko

A Behavior-Based Approach to Securing Email Systems 57
S.J. Stolfo, S. Hershkop, K. Wang, O. Nimeskern, and C.-W. Hu

Real-Time Intrusion Detection with Emphasis on Insider Attacks 82
S. Upadhyaya

Mathematical Models and Architectures for Computer Network Security

Relating Process Algebras and Multiset Rewriting for Immediate Decryption Protocols 86
S. Bistarelli, I. Cervesato, G. Lenzini, and F. Martinelli

GRID Security Review 100
L. Gymnopoulos, S. Dritsas, S. Gritzalis, and C. Lambrinoudakis

A Knowledge-Based Repository Model for Security Policies Management .. 112
S. Kokolakis, C. Lambrinoudakis, and D. Gritzalis

Symbolic Partial Model Checking for Security Analysis 122
F. Martinelli

Rule-Based Systems Security Model 135
M. Smirnov

Logical Resolving for Security Evaluation 147
P.D. Zegzhda, D.P. Zegzhda, and M.O. Kalinin

Intrusion Detection

Enhanced Correlation in an Intrusion Detection Process 157
S. Benferhat, F. Autrel, and F. Cuppens

Safeguarding SCADA Systems with Anomaly Detection 171
J. Bigham, D. Gamez, and N. Lu

Experiments with Simulation of Attacks against Computer Networks 183
I. Kotenko and E. Man'kov

Detecting Malicious Codes by the Presence
of Their "Gene of Self-replication" 195
V.A. Skormin, D.H. Summerville, and J.S. Moronski

Automatic Generation of Finite State Automata for Detecting Intrusions
Using System Call Sequences 206
K. Wee and B. Moon

Public Key Distribution, Authentication, Access Control

Distributed Access Control: A Logic-Based Approach 217
S. Barker

Advanced Certificate Status Protocol 229
D.H. Yum, J.E. Kang, and P.J. Lee

Key History Tree: Efficient Group Key Management
with Off-Line Members 241
A. Lain and V. Borisov

A Certificate Status Checking Protocol for the Authenticated Dictionary . . 255
J.L. Munoz, J. Forne, O. Esparza, and M. Soriano

Context-Dependent Access Control
for Web-Based Collaboration Environments with Role-Based Approach . . . 267
R. Wolf and M. Schneider

Cryptography

A Signcryption Scheme Based on Secret Sharing Technique 279
M. Al-Ibrahim

A Zero-Knowledge Identification Scheme
Based on an Average-Case NP-Complete Problem 289
P. Caballero-Gil and C. Hernández-Goya

Linear Cryptanalysis on SPECTR-H64
with Higher Order Differential Property 298
Y.D. Ko, D.J. Hong, S.H. Hong, S.J. Lee, and J.L. Lim

Achieveability of the Key-Capacity in a Scenario of Key Sharing by Public Discussion and in the Presence of Passive Eavesdropper 308
V. Korzhik, V. Yakovlev, and A. Sinuk

On Cipher Design Based on Switchable Controlled Operations 316
N.A. Moldovyan

Elliptic Curve Point Multiplication 328
A. Rostovtsev and E. Makhovenko

Encryption and Data Dependent Permutations: Implementation Cost and Performance Evaluation 337
N. Sklavos, A.A. Moldovyan, and O. Koufopavlou

Steganography

Simulation-Based Exploration of SVD-Based Technique for Hidden Communication by Image Steganography Channel 349
V. Gorodetsky and V. Samoilov

Detection and Removal of Hidden Data in Images Embedded with Quantization Index Modulation 360
K. Zhang, S. Wang, and X. Zhang

Digital Watermarking under a Filtering and Additive Noise Attack Condition 371
V. Korzhik, G. Morales-Luna, I. Marakova, and C. Patiño-Ruvalcaba

Data Hiding in Digital Audio by Frequency Domain Dithering 383
S. Wang, X. Zhang, and K. Zhang

Steganography with Least Histogram Abnormality 395
X. Zhang, S. Wang, and K. Zhang

Multi-bit Watermarking Scheme Based on Addition of Orthogonal Sequences 407
X. Zhang, S. Wang, and K. Zhang

Short Papers

Authentication of Anycast Communication 419
M. Al-Ibrahim and A. Cerny

Two-Stage Orthogonal Network Incident Detection for the Adaptive Coordination with SMTP Proxy 424
R. Ando and Y. Takefuji

Construction of the Covert Channels 428
A. Grusho and E. Timonina

Privacy and Data Protection in Electronic Communications 432
L. Mitrou and K. Moulinos

Multiplier for Public-Key Cryptosystem Based on Cellular Automata 436
H.S. Kim and S.H. Hwang

A Game Theoretic Approach to Analysis and Design of Survivable and Secure Systems and Protocols 440
S. Kumar and V. Marbukh

Alert Triage on the ROC 444
F.J. Martin and E. Plaza

Fast Ciphers for Cheap Hardware: Differential Analysis of SPECTR-H64 . . 449
N.D. Goots, B.V. Izotov, A.A. Moldovyan, and N.A. Moldovyan

Immunocomputing Model of Intrusion Detection 453
Y. Melnikov and A. Tarakanov

Agent Platform Security Architecture 457
G. Santana, L.B. Sheremetov, and M. Contreras

Support Vector Machine Based ICMP Covert Channel Attack Detection . . 461
T. Sohn, T. Noh, and J. Moon

Computer Immunology System with Variable Configuration 465
S.P. Sokolova and R.S. Ivlev

Author Index 469