

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Igor Kotenko Victor Skormin (Eds.)

Computer Network Security

6th International Conference on Mathematical
Methods, Models and Architectures for
Computer Network Security, MMM-ACNS 2012
St. Petersburg, Russia, October 17-19, 2012
Proceedings



Springer

Volume Editors

Igor Kotenko

St. Petersburg Institute for Informatics and Automation

Russian Academy of Science

39, 14-th Liniya

St. Petersburg, 199178, Russia

E-mail: ivkote@comsec.spb.ru

Victor Skormin

Binghamton University (SUNY)

Binghamton, NY 13902, USA

E-mail: vskormin@binghamton.edu

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-33703-1

e-ISBN 978-3-642-33704-8

DOI 10.1007/978-3-642-33704-8

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012947925

CR Subject Classification (1998): C.2.0, K.6.5, K.4.4, E.3, D.4.6, C.2.3-4, H.2.7-8, C.5.3, J.1

LNCS Sublibrary: SL 5 – Computer Communication Networks and Telecommunications

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains papers presented at the 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2012) held in St. Petersburg, Russia, during October 17–19, 2012. The conference was organized by the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) in cooperation with Binghamton University (SUNY).

The previous international conferences “Mathematical Methods, Models and Architectures for Computer Networks Security” (MMM-ACNS 2001, MMM-ACNS 2003, MMM-ACNS 2005, MMM-ACNS 2007, and MMM-ACNS 2010), organized by SPIIRAS and Binghamton University (SUNY) and supported by the European Office of Aerospace Research and Development USAF, the US Office of Naval Research Global, and the Russian Foundation for Basic Research, were successful. These conferences demonstrated the high interest of the international scientific community in the theoretical and practical aspects of computer network security.

MMM-ACNS 2012 provided the next international forum for sharing original research results among specialists in fundamental and applied problems of computer network security. A total of 44 papers from 12 countries were submitted to MMM-ACNS 2012. Fourteen papers were selected as regular and 8 as short presentations (32% of acceptance for full papers).

Seven technical sessions were organized, namely: applied cryptography and security protocols; access control and information protection; security policies; security event and information management; intrusion prevention, detection, and response; anti-malware techniques; and security modeling and cloud security. The MMM-ACNS 2012 program was enriched by invited papers presented by four distinguished invited speakers: Ben Livshits (Microsoft Research and University of Washington, USA), Fabio Martinelli (Institute of Informatics and Telematics, National Research Council, Italy), Angelos Stavrou (Mason University, USA), and Bhavani Thuraisingham (University of Texas at Dallas, USA).

The success of the conference was assured by the team effort 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 conference and all authors of the submitted papers. We are grateful to our sponsors: European Office of Aerospace Research and Development (EOARD) of the US Air Force and the US Office of Naval Research Global (ONRGlobal).

We wish to express our gratitude to Springer’s LNCS team managed by Alfred Hofmann for their help and cooperation.

October 2012

Igor Kotenko
Victor Skormin

Organization

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

Igor Kotenko	St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Russia
Victor Skormin	Binghamton University, USA

Program Committee

Fabrizio Baiardi	University of Pisa, Italy
Cataldo Basile	Politecnico di Torino, Italy
Julien Bourgeois	University of Franche-Comte, France
Mariano Ceccato	Fondazione Bruno Kessler, Italy
David Chadwick	University of Kent, UK
Shiu-Kai Chin	Syracuse University, USA
Christian Collberg	University of Arizona, USA
Miguel Pupo Correia	Instituto Superior Técnico, Portugal
Bruno Crispo	University of Trento, Italy
Frédéric Cuppens	Télécom Bretagne, France
Dipankar Dasgupta	University of Memphis, USA
Changyu Dong	University of Strathclyde, UK
Dennis Gamayunov	Moscow State University, Russia
Dieter Gollmann	Technical University of Hamburg-Harburg, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Alexander Grusho	Moscow State University, Russia
Ming-Yuh Huang	Northwest Security Institute, USA
Andrew Hutchison	T-Systems, South Africa
Sushil Jajodia	George Mason University, USA
Angelos Keromytis	Columbia University, USA
Alexey Kirichenko	F-Secure, Finland
Victor Korneev	Federal Enterprise “R&D Institute “Kvant”, Russia
Hanno Langweg	Gjøvik University College, Norway
Pavel Laskov	University of Tübingen, Germany

Peeter Laud	Cybernetica AS and University of Tartu, Estonia
Ben Livshits	Microsoft Research and University of Washington, USA
Javier Lopez	University of Malaga, Spain
Antonio Maña	University of Malaga, Spain
Fabio Martinelli	Institute of Informatics and Telematics, National Research Council, Italy
Gregorio Martinez	University of Murcia, Spain
Fabio Massacci	University of Trento, Italy
Catherine Meadows	Naval Research Laboratory, USA
Stig Mjølunes	Norwegian University of Science and Technology, Norway
Nikolay Moldovyan	SPIIRAS, Russia
Wojciech Molisz	Gdansk University of Technology, Poland
Greg Morrisett	Harvard University, USA
Haris Mouratidis	University of East London, UK
Evgenia Novikova	SPIIRAS, Russia
Vladimir Oleshchuk	University of Agder, Norway
Ludovic Pietre-Cambacedes	EDF, France
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Roland Rieke	Fraunhofer Institute for Secure Information Technology SIT, Germany
Luigi Romano	University of Naples Parthenope, Italy
Andrzej Rucinski	University of New Hampshire, USA
Peter Ryan	University of Luxembourg, Luxembourg
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Ahmad-Reza Sadeghi	TU Darmstadt and Fraunhofer Institute for Secure Information Technology SIT, Germany
Igor Saenko	SPIIRAS, Russia
Francoise Sailhan	CNAM, France
Pierangela Samarati	University of Milan, Italy
Ravi Sandhu	George Mason University and NSD Security, USA
Fred Schneider	Cornell University, USA
Michael Smirnov	Fraunhofer FOKUS, Germany
Angelos Stavrou	Mason University, USA
Nadia Tawbi	Laval University, Canada
Bhavani Thuraisingham	University of Texas at Dallas, USA
Bill Tsoumas	Athens University of Economics and Business, Greece
Shambhu Upadhyaya	University at Buffalo, USA
Paulo Verissimo	University of Lisbon, Portugal
Peter Zegzhda	St. Petersburg Polytechnical University, Russia

Reviewers

Fabrizio Baiardi	University of Pisa, Italy
Cataldo Basile	Politecnico di Torino, Italy
Luciano Bello	Chalmers University of Technology, Sweden
Julien Bourgeois	University of Franche-Comté, France
Mariano Ceccato	Fondazione Bruno Kessler, Italy
David Chadwick	University of Kent, UK
Shiu-Kai Chin	Syracuse University, USA
Christian Collberg	University of Arizona, USA
Miguel Pupo Correia	Instituto Superior Técnico, Portugal
Frédéric Cuppens	Télécom Bretagne, France
Changyu Dong	University of Strathclyde, UK
Dennis Gamayunov	Moscow State University, Russia
Dieter Gollmann	Technical University of Hamburg-Harburg, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Alexander Grusho	Moscow State University, Russia
Ming-Yuh Huang	Northwest Security Institute, USA
Andrew Hutchison	T-Systems, South Africa
Sushil Jajodia	George Mason University, USA
Angelos Keromytis	Columbia University, USA
Alexey Kirichenko	F-Secure, Finland
Victor Korneev	Federal Enterprise “R&D Institute “Kvant”, Russia
Hanno Langweg	Gjøvik University College, Norway
Pavel Laskov	University of Tübingen, Germany
Peeter Laud	Cybernetica AS and University of Tartu, Estonia
Ben Livshits	Microsoft Research and University of Washington, USA
Javier Lopez	University of Malaga, Spain
Antonio Maña	University of Malaga, Spain
Fabio Martinelli	Institute of Informatics and Telematics, National Research Council, Italy
Gregorio Martinez	University of Murcia, Spain
Fabio Massacci	University of Trento, Italy
Catherine Meadows	Naval Research Laboratory, USA
Stig Mjølsnes	Norwegian University of Science and Technology, Norway
Nikolay Moldovyan	SPIIRAS, Russia
Wojciech Molisz	Gdansk University of Technology, Poland
Greg Morrisett	Harvard University, USA
Haris Mouratidis	University of East London, UK
Evgenia Novikova	SPIIRAS, Russia
Vladimir Oleshchuk	University of Agder, Norway

Ludovic Pietre-Cambacedes	EDF, France
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Willard Rafnsson	Chalmers University of Technology, Sweden
Roland Rieke	Fraunhofer Institute for Secure Information Technology SIT, Germany
Luigi Romano	University of Naples Parthenope, Italy
Andrzej Rucinski	University of New Hampshire, USA
Peter Ryan	University of Luxembourg, Luxembourg
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Ahmad-Reza Sadeghi	TU Darmstadt and Fraunhofer Institute for Secure Information Technology SIT, Germany
Igor Saenko	SPIIRAS, Russia
Francoise Sailhan	CNAM, France
Pierangela Samarati	University of Milan, Italy
Ravi Sandhu	George Mason University and NSD Security, USA
Fred Schneider	Cornell University, USA
Michael Smirnov	Fraunhofer FOKUS, Germany
Angelos Stavrou	Mason University, USA
Nadia Tawbi	Laval University, Canada
Bhavani Thuraisingham	University of Texas at Dallas, USA
Bill Tsoumas	Athens University of Economics and Business, Greece
Shambhu Upadhyaya	University at Buffalo, USA
Paulo Verissimo	University of Lisbon, Portugal
Peter Zegzhda	St. Petersburg Polytechnical University, Russia

Table of Contents

Invited Papers

Finding Malware on a Web Scale.....	1
<i>Benjamin Livshits</i>	
Exposing Security Risks for Commercial Mobile Devices	3
<i>Zhaohui Wang, Ryan Johnson, Rahul Murruria, and Angelos Stavrou</i>	
From Qualitative to Quantitative Enforcement of Security Policy.....	22
<i>Fabio Martinelli, Ilaria Matteucci, and Charles Morisset</i>	
Design and Implementation of a Cloud-Based Assured Information Sharing System	36
<i>Tyrone Cadenhead, Murat Kantarcioglu, Vaibhav Khadilkar, and Bhavani Thuraisingham</i>	

Applied Cryptography and Security Protocols

Optimization of Key Distribution Protocols Based on Extractors for Noisy Channels within Active Adversaries	51
<i>Victor Yakovlev, Valery Korzhik, Mihail Bakaev, and Guillermo Morales-Luna</i>	
A Vulnerability in the UMTS and LTE Authentication and Key Agreement Protocols	65
<i>Joe-Kai Tsay and Stig F. Mjølunes</i>	
Blind 384-bit Digital Signature Scheme	77
<i>Alexandr Moldovyan, Nikolay Moldovyan, and Evgenia Novikova</i>	

Access Control and Information Protection

RABAC: Role-Centric Attribute-Based Access Control.....	84
<i>Xin Jin, Ravi Sandhu, and Ram Krishnan</i>	
Trust-Aware RBAC	97
<i>Vladimir Oleshchuk</i>	
Alternative Mechanisms for Information Security.....	108
<i>Alexander Grusho, Nick Grusho, and Elena Timonina</i>	

Security Policies

Enforcing Information Flow Policies by a Three-Valued Analysis	114
<i>Josée Desharnais, Erwanne P. Kanyabwero, and Nadia Tawbi</i>	
Towards the Orchestration of Secured Services under Non-disclosure Policies	130
<i>Tigran Avanesov, Yannick Chevalier, Michaël Rusinowitch, and Mathieu Turuani</i>	
An Approach for Network Information Flow Analysis for Systems of Embedded Components	146
<i>Andrey Chechulin, Igor Kotenko, and Vasily Desnitsky</i>	

Security Event and Information Management

Individual Countermeasure Selection Based on the Return On Response Investment Index	156
<i>Gustavo Gonzalez Granadillo, Hervé Débar, Grégoire Jacob, Chrystel Gaber, and Mohammed Achemlal</i>	
Security and Reliability Requirements for Advanced Security Event Management	171
<i>Roland Rieke, Luigi Coppolino, Andrew Hutchison, Elsa Prieto, and Chrystel Gaber</i>	
Model-Based Security Event Management	181
<i>Julian Schütte, Roland Rieke, and Timo Winkelvos</i>	

Intrusion Prevention, Detection, and Response

Using Behavioral Modeling and Customized Normalcy Profiles as Protection against Targeted Cyber-Attacks	191
<i>Andrey Dolgikh, Tomas Nykodym, Victor Skormin, and Zachary Birnbaum</i>	
Limitation of Honeypot/Honeynet Databases to Enhance Alert Correlation	203
<i>Yosra Ben Mustapha, Hervé Débar, and Grégoire Jacob</i>	
Stochastic Model of Interaction between Botnets and Distributed Computer Defense Systems	218
<i>Dmitry P. Zegzhda and Tatiana V. Stepanova</i>	

Anti-malware Techniques

Malware Characterization Using Behavioral Components	226
<i>Chaitanya Yavvari, Arnur Tokhtabayev, Huzefa Rangwala, and Angelos Stavrou</i>	
MADAM: A Multi-level Anomaly Detector for Android Malware	240
<i>Gianluca Dini, Fabio Martinelli, Andrea Saracino, and Daniele Sgandurra</i>	
Using Low-Level Dynamic Attributes for Malware Detection Based on Data Mining Methods	254
<i>Dmitry Komashinskiy and Igor Kotenko</i>	

Security Modeling and Cloud Security

Configuration-Based Approach to Embedded Device Security	270
<i>Vasily Desnitsky, Igor Kotenko, and Andrey Chechulin</i>	
A Study of Entropy Sources in Cloud Computers: Random Number Generation on Cloud Hosts	286
<i>Brendan Kerrigan and Yu Chen</i>	
Security Modeling of Grid Systems Using Petri Nets	299
<i>Peter D. Zegzhda, Dmitry P. Zegzhda, Maxim O. Kalinin, and Artem S. Konoplev</i>	
Using Graph Theory for Cloud System Security Modeling	309
<i>Peter D. Zegzhda, Dmitry P. Zegzhda, and Alexey V. Nikolskiy</i>	
Author Index	319