

2009 Fourth International Conference on Internet Monitoring and Protection

(ICIMP)

**Venice, Italy
24 – 28 May 2009**

Editors:

**Sorin Georgescu
Seppo Heikkinen**

Manuela Popescu



**IEEE Catalog Number: CFP0954C-PRT
ISBN: 978-1-4244-3839-6**

**Copyright © 2009 by the Institute of Electrical and Electronic Engineers, Inc
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

******This publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number: CFP0954C-PRT
ISBN 13: 978-1-4244-3839-6

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com

2009 Fourth International Conference on Internet Monitoring and Protection

ICIMP 2009

Table of Contents

Preface

Program Committee

Reviewers

ICIMP 1: TRASI

Effective Change Detection in Large Repositories of Unsolicited Traffic	1
<i>Ejaz Ahmed, Andrew Clark, and George Mohay</i>	
A Technique for Detecting New Attacks in Low-Interaction Honeypot Traffic	7
<i>S. Almotairi, A. Clark, G. Mohay, and J. Zimmermann</i>	
Framework for Zombie Detection Using Neural Networks	14
<i>Paulo Salvador, António Nogueira, Ulisses França, and Rui Valadas</i>	
Scalable and Density-Aware Measurement Strategies for Overlay Networks	21
<i>Go Hasegawa and Masayuki Murata</i>	

ICIMP 2: USSAF

Towards Developing Secure Video Surveillance Systems over IP	27
<i>Bogdan Groza, Ioan Silea, Dragos Pop, and Victor-Valeriu Patriciu</i>	
Development of Social Networks in Email Communication	34
<i>Kamil Malinka and Jiří Schäfer</i>	
Security in Peer-to-Peer Networks: Empiric Model of File Diffusion in BitTorrent	39
<i>Jiří Schäfer and Kamil Malinka</i>	
Enhancing Privacy Implementations of Database Enquiries	45
<i>Florian Kammüller and Reiner Kammüller</i>	

ICIMP 3: IPERF, RTSEC, EMDRM, and SYVUL

An Empirical Evaluation on Semantic Search Performance of Keyword-Based and Semantic Search Engines: Google, Yahoo, Msn and Hakia	51
<i>Duygu Tümer, Mohammad Ahmed Shah, and Yiltan Bitirim</i>	
Extraction of Parameters from Well Managed Networked System in Access Control	56
<i>Akira Kanaoka, Masahiko Katoh, Nobukatsu Toudou, and Eiji Okamoto</i>	
Domain Based Content Sharing in Digital Home	62
<i>Jungsoo Lee, Junghyun Kim, Jihyun Park, and Kisong Yoon</i>	
Where Only Fools Dare to Tread: An Empirical Study on the Prevalence of Zero-Day Malware	66
<i>Håvard Vegge, Finn Michael Halvorsen, Rune Walsø Nergård, Martin Gilje Jaatun, and Jostein Jensen</i>	

ICIMP 4: REPORT and BIOTEC

Behavior-Based Proactive Detection of Unknown Malicious Codes	72
<i>Jianguo Ding, Jian Jin, Pascal Bouvry, Yongtao Hu, and Haibing Guan</i>	
IT Security in Banking - Processes, Practical Experiences and Lessons Learned	78
<i>Igor Podebrad and Martin Drotleff</i>	
Usability of Visual Evoked Potentials as Behavioral Characteristics for Biometric Authentication	84
<i>Kamil Malinka</i>	
Cognitive-Based Biometrics System for Static User Authentication	90
<i>Omar Hamdy and Issa Traoré</i>	

ICIMP 5: RISK, SYDIA, and WIP

Security Assurance Metrics and Aggregation Techniques for IT Systems	98
<i>Moussa Ouedraogo, Haralambos Mouratidis, Djamel Khadraoui, and Eric Dubois</i>	
Fuzzy Heuristic Design for Diagnosis of Web-Based Vulnerabilities	103
<i>Deepak Subramanian, Ha Thanh Le, and Peter Kok Keong Loh</i>	
A Probe Framework for Monitoring Embedded Real-Time Systems	109
<i>Markku Pollari and Teemu Kanstrén</i>	
Information Security Management is Not Only Risk Management	116
<i>Igli Tashi and Solange Ghernouti-Hélie</i>	

ICIMP 6: MONIT

Are Smaller Packets Less Likely to Be Lost?	124
<i>Joel Sommers, Victor Omwando, and Fred Sisenda</i>	
Assolo, a New Method for Available Bandwidth Estimation	130
<i>Emanuele Goldoni, Giuseppe Rossi, and Alberto Torelli</i>	

Fast Dynamics in Internet Topology: Observations and First Explanations	137
<i>Clémence Magnien, Frédéric Ouédraogo, Guillaume Valadon, and Matthieu Latapy</i>	
Rating Autonomous Systems	143
<i>Laurent Zimmerli, Bernhard Tellenbach, Arno Wagner, and Bernhard Plattner</i>	

Author Index