2009 Fourth International Conference on Internet Monitoring and Protection

ICIMP 2009

Table of Contents

Preface........................................................................................................................................................viii
Program Committee.....................................................................................................................................x
Reviewers...................................................................................................................................................xiii

ICIMP 1: TRASI

Effective Change Detection in Large Repositories of Unsolicited Traffic .....................................................1
\textit{Ejaz Ahmed, Andrew Clark, and George Mohay}

A Technique for Detecting New Attacks in Low-Interaction Honeypot Traffic ..............................................7
\textit{S. Almotairi, A. Clark, G. Mohay, and J. Zimmermann}

Framework for Zombie Detection Using Neural Networks ..........................................................................14
\textit{Paulo Salvador, António Nogueira, Ulisses França, and Rui Valadas}

Scalable and Density-Aware Measurement Strategies for Overlay Networks ............................................21
\textit{Go Hasegawa and Masayuki Murata}

ICIMP 2: USSAF

Towards Developing Secure Video Surveillance Systems over IP .................................................................27
\textit{Bogdan Groza, Ioan Silea, Dragos Pop, and Victor-Valeriu Patriciu}

Development of Social Networks in Email Communication ........................................................................34
\textit{Kamil Malinka and Jiří Schäfer}

Security in Peer-to-Peer Networks: Empiric Model of File Diffusion in BitTorrent ....................................39
\textit{Jiří Schäfer and Kamil Malinka}

Enhancing Privacy Implementations of Database Enquiries ....................................................................45
\textit{Florian Kammüller and Reiner Kammüller}
## 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

*Duygu Tümer, Mohammad Ahmed Shah, and Yıltan Bitirim*

Extraction of Parameters from Well Managed Networked System in Access Control ........................................................................................................................................................56

*Akira Kanaoka, Masahiko Katoh, Nobukatsu Toudou, and Eiji Okamoto*

Domain Based Content Sharing in Digital Home ..........................................................................................................................62

*Jungsoo Lee, Junghyun Kim, Jihyun Park, and Kisong Yoon*

Where Only Fools Dare to Tread: An Empirical Study on the Prevalence of Zero-Day Malware ..................................................................................................................................66

*Håvard Vegge, Finn Michael Halvorsen, Rune Walsø Nergård, Martin Gilje Jaatun, and Jostein Jensen*

## ICIMP 4: REPORT and BIOTEC

Behavior-Based Proactive Detection of Unknown Malicious Codes ..........................................................72

*Jianguo Ding, Jian Jin, Pascal Bouvry, Yongtao Hu, and Haibing Guan*

IT Security in Banking - Processes, Practical Experiences and Lessons Learned .......................................................................................................................................................78

*Igor Podebrad and Martin Drotleff*

Usability of Visual Evoked Potentials as Behavioral Characteristics for Biometric Authentication ..................................................................................................................................................84

*Kamil Malinka*

Cognitive-Based Biometrics System for Static User Authentication ........................................................................................................................90

*Omar Hamdy and Issa Traoré*

## ICIMP 5: RISK, SYDIA, and WIP

Security Assurance Metrics and Aggregation Techniques for IT Systems ...........................................................98

*Moussa Ouedraogo, Haralambos Mouratidis, Djamel Khadraoui, and Eric Dubois*

Fuzzy Heuristic Design for Diagnosis of Web-Based Vulnerabilities ..........................................................................................................................103

*Deepak Subramanian, Ha Thanh Le, and Peter Kok Keong Loh*

A Probe Framework for Monitoring Embedded Real-Time Systems ..........................................................................................................................109

*Markku Pollari and Teemu Kanstrén*

Information Security Management is Not Only Risk Management ..........................................................................................................................116

*Igli Tashi and Solange Ghernouti-Hélé*

## ICIMP 6: MONIT

Are Smaller Packets Less Likely to Be Lost? ...........................................................................................................................124

*Joel Sommers, Victor Omwando, and Fred Sisenda*

Assolo, a New Method for Available Bandwidth Estimation ..........................................................................................................................130

*Emanuele Goldoni, Giuseppe Rossi, and Alberto Torelli*