

Proceedings

**The Third International
Conference on Internet
Monitoring and Protection
ICIMP 2008**

**29 June - 5 July 2008
Bucharest, Romania**



**Los Alamitos, California
Washington • Tokyo**



The Third International Conference on Internet Monitoring and Protection

ICIMP 2008

Table of Contents

| | |
|-----------------|------|
| Preface..... | viii |
| Committees..... | ix |

ICIMP1: MONIT I

| | |
|----------------------------------------------------------------------------------------------|----|
| Dynamic Verification and Control of Mobile Peer-to-Peer Systems | 1 |
| <i>George Spanoudakis, Christos Kloukinas, and Kelly Androutsopoulos</i> | |
| HIDDEN: Hausdorff Distance Based Intrusion Detection Approach DEdicated to Networks | 11 |
| <i>Yann Labit and Johan Mazel</i> | |
| Mouse Trapping: A Flow Data Reduction Method | 17 |
| <i>Sven Anderson and Dieter Hogrefe</i> | |
| Large-Scale Video Surveillance Systems: New Performance Parameters and Metrics | 23 |
| <i>S. Sutor, F. Matussek, F. Kruse, K. Kraus, and R. Reda</i> | |

ICIMP2: MONIT II

| | |
|--------------------------------------------------------------------------|----|
| Impact of Traffic Mix and Packet Sampling on Anomaly Visibility | 31 |
| <i>Bernhard Tellenbach, Daniela Brauckhoff, and Martin May</i> | |
| Traffic Anomaly Detection at Fine Time Scales with Bayes Nets | 37 |
| <i>Jeff Kline, Sangnam Nam, Paul Barford, David Plonka, and Amos Ron</i> | |
| Towards a User-Centric Identity-Usage Monitoring System | 47 |
| <i>Daisuke Mashima and Mustaque Ahamad</i> | |
| VOC Based Key Quality Indicators for High-Speed Internet Service | 53 |
| <i>Dae-Woo Kim, Hyun-Min Lim, Jae-Hyoung Yoo, and 'Sang-Ha Kim</i> | |

ICIMP3: RTSEC I

| | |
|------------------------------------------------------------------------------------------------------|----|
| Specification-Based Denial-of-Service Detection for SIP Voice-over-IP Networks | 59 |
| <i>Sven Ehlert, Chengjian Wang, Thomas Magedanz, and Dorgham Sisalem</i> | |
| Zombie Identification Port | 67 |
| <i>Pedro R. M. Inácio, Joao V. P. Gomes, Mário M. Freire, Manuela Pereira, and Paulo P. Monteiro</i> | |
| Peer-to-Peer Networks Security | 74 |
| <i>J. Schäfer, K. Malinka, and P. Hanáček</i> | |

ICIMP4: RTSEC II

| | |
|----------------------------------------------------------------------------------------------------------------|----|
| A Threat-Aware Signature Based Intrusion-Detection Approach for Obtaining Network-Specific Useful Alarms | 80 |
| <i>Subramanian Neelakantan and Shrisha Rao</i> | |
| Towards Fast Detecting Intrusions: Using Key Attributes of Network Traffic | 86 |
| <i>Wei Wang, Sylvain Gombault, and Thomas Guyet</i> | |
| Cryptographic Authentication on the Communication from an 8051 Based Development Board over UDP | 92 |
| <i>Bogdan Groza, Pal-Stefan Murvay, Ioan Silea, and Tiberiu Ionica</i> | |
| NIVSS: A Nearly Indestructible Video Surveillance System | 98 |
| <i>F. Matussek, S. Sutor, K. Kraus, F. Kruse, and R. Reda</i> | |

ICIMP5: SYDIA

| | |
|-------------------------------------------------------------------------------|-----|
| An Empirical Study on Data Center System Failure Diagnosis | 103 |
| <i>Montri Wiboonrat</i> | |
| A Dangerousness-Based Investigation Model for Security Event Management | 109 |
| <i>V. Legrand, R. State, and L. Paffumi</i> | |
| A Merge Method for Decentralized Discrete-Event Fault Diagnosis | 119 |
| <i>He-xuan Hu, Anne-lise Gehin, and Mireille Bayart</i> | |

ICIMP6: RISK & TRUST

| | |
|------------------------------------------------------------------------------------------------------|-----|
| A Holistic, Collaborative, Knowledge-Sharing Approach for Information Security Risk Management | 125 |
| <i>Ekaterini Papadaki, Despina Polemi, and Dimitrios Kon/nos Damilos</i> | |
| Efficient Security Measurements and Metrics for Risk Assessment | 131 |
| <i>I. Tashi and S. Ghernaoui-Hélie</i> | |
| An Access Service Scheme with Anonymity for Ubiquitous Computing Based on Mobile IPv6 | 139 |
| <i>Chou-Chen Yang, Gwoboa Horng, and Jing-Wen Li</i> | |
| Establishing a Secure Peer Identity Association Using IMS Architecture | 145 |
| <i>Seppo Heikkinen</i> | |

| | |
|-------------------------------------------------------------------------------------------------|-----|
| A Near Real-Time System for Security Assurance Assessment | 152 |
| <i>Nguyen Pham, Loic Baud, Patrick Bellot, and Michel Riguidel</i> | |
| ICIMP7: USSAF | |
| An Evaluation of Major Image Search Engines on Various Query Topics | 161 |
| <i>Ece Çakir, Hüseyin Bahçeci, and Yiltan Bitirim</i> | |
| A Classification of Security Feedback Design Patterns for Interactive Web Applications | 166 |
| <i>Jaime Munoz-Arteaga, Ricardo Mendoza González, and Jean Vanderdonckt</i> | |
| An Empirical Analysis of RS Steganalysis | 172 |
| <i>Sathiamoorthy Manoharan</i> | |
| Identity Management in Mobile Ubiquitous Environments | 178 |
| <i>Tor Anders Johansen, Ivar Jorstad, and Do van Thanh</i> | |
| Author Index | 185 |