

Proceedings



Second International Conference on Internet Monitoring and Protection

ICIMP 2007

1-5 July 2007 • San Jose, California



Los Alamitos, California
Washington • Tokyo



Proceedings



ICIMP 2007

Table of Contents

Preface **Committees**

ICIMP 1

| | |
|--|----|
| Enriched Diagnosis and Investigation Models for Security Event Correlation | 1 |
| <i>Véronique Legrand and Stéphane Ubéda</i> | |
| BTM—An Automated Rule-Based BT Monitoring System for Piracy Detection | 9 |
| <i>K. P. Chow, K. Y. Cheng, L. Y. Man, Pierre K. Y. Lai, Lucas C. K. Hui, C. F. Chong, K. H. Pun, W. W. Tsang, H. W. Chan, and S. M. Yiu</i> | |
| Phishing Phishers—Observing and Tracing Organized Cybercrime | 15 |
| <i>Dominik Birk, Sebastian Gajek, Felix Gröbert, and Ahmad-Reza Sadeghi</i> | |
| An Investigation of Cybercrime-Related Online Search Behaviors vs General Search Behavior..... | 21 |
| <i>Jingguo Wang, Nan Xiao, and H. Raghav Rao</i> | |
| Monitoring Architecture for Lawful Interception in VoIP Networks | 27 |
| <i>Balamurugan Karpagavinayagam, Radu State, and Olivier Festor</i> | |

ICIMP 2

| | |
|--|----|
| Large Scale Activity Monitoring for Distributed Honeynets..... | 33 |
| <i>Jerome François, Radu State, and Olivier Festor</i> | |

| | |
|---|----|
| Visualisation of Network Traffic using Dynamic Co-occurrence Matrices | 39 |
| <i>Thorsten Kisner, Alex Essoh, and Firoz Kaderali</i> | |
| Improving Routing Security Using a Decentralized Public Key Distribution Algorithm..... | 45 |
| <i>Jeremy Goold and Mark Clement</i> | |
| A Comparison of SYN Flood Detection Algorithms..... | 53 |
| <i>Matt Beaumont-Gay</i> | |
| IPv6 Anomaly Traffic Monitoring with IPFIX..... | 59 |
| <i>Youngseok Lee, Seongho Shin, Soonbyoung Choi, and Hyeon-gu Son</i> | |

ICIMP 3

| | |
|---|----|
| A Management Platform for Tracking Cyber Predators in Peer-to-Peer Networks..... | 65 |
| <i>Remi Badonnel, Radu State, Isabelle Chrissent, and Olivier Festor</i> | |
| Fraud/Privacy Protection in Anonymous Auction..... | 71 |
| <i>Hassan Kazem, Qadeer Hasan, and Rafiqul Zaman Khan</i> | |
| Emergency Alerts as RSS Feeds with Interdomain Authorization | 76 |
| <i>Filippo Gioachin, Ravinder Shankesi, Michael J. May, Carl A. Gunter, and Wook Shin</i> | |
| Inferring Available Bandwidth of Overlay Network Paths Based on Inline Network Measurement | 84 |
| <i>Cao Le Thanh Man, Go Hasegawa, and Masayuki Murata</i> | |

ICIMP 4

| | |
|--|-----|
| Performance Analysis in IP over WDM Networks..... | 90 |
| <i>Cebraïl Taşkin</i> | |
| On the End-to-End Delay Analysis of the IEEE 802.11 Distributed Coordination Function..... | 96 |
| <i>J. S. Vardakas, I. Papanagioutou, M. D. Logothetis, and S. A. Kotsopoulos</i> | |
| Automated Discovery of Performance Envelopes..... | 101 |
| <i>James Bouhana and Mike Tsykin</i> | |
| Toward the Use of Automated Static Analysis Alerts for Early Identification of Vulnerability- and Attack-Prone Components | 108 |
| <i>Michael Gegick and Laurie Williams</i> | |

ICIMP 5

| | |
|--|-----|
| Protocol to Support Multi-domain Auditing of Internet-Based Transport Services | 114 |
| <i>Frank Eyermann and Burkhard Stiller</i> | |

| | |
|---|-----|
| Efficient Probing Techniques for Fault Diagnosis..... | 122 |
| <i>Maitreya Natu and Adarshpal S. Sethi</i> | |
| Modeling End-to-End Delay Using Pareto Distribution..... | 128 |
| <i>Wei Zhang and Jingsha He</i> | |
| An Experimental Approach to Integrating NetFlow Flow-Level Records and NLANR Packet-Level Traces | 132 |
| <i>Chi Zhang, Bin Liu, Xun Su, Heidi Alvarez, and Julio Ibarra</i> | |
| On the Penetration of Business Networks by P2P File Sharing..... | 138 |
| <i>Kevin Lee, Danny Hughes, and James Walkerdine</i> | |

ICIMP 6

| | |
|---|-----|
| Non-repudiable Service Usage with Host Identities | 144 |
| <i>Seppo Heikkinen</i> | |
| Smurf-Based Distributed Denial of Service (DDoS) Attack Amplification in Internet..... | 150 |
| <i>Sanjeev Kumar</i> | |
| State of the Art Review of the Existing Bayesian-Network Based Approaches to Trust and Reputation Computation..... | 155 |
| <i>Farookh Khadeer Hussain, Elizabeth Chang, and Omar Khadeer Hussain</i> | |

ICGD&BC 1

| | |
|--|-----|
| Business Continuity Plan Design: 8 Steps for Getting Started Designing a Plan | 160 |
| <i>Richard J. Kepenach</i> | |
| Active Biometric Cryptography (ABC): Key Generation Using Feature and Parametric Aggregation..... | 164 |
| <i>Christopher R. Costanzo</i> | |
| X.500 Type Databases for Flexible and Highly Available Common and Logically Centralized User Data Storage in Telecommunication..... | 170 |
| <i>W. Haidegger</i> | |
| Project ENSAYO: A Virtual Emergency Operations Center for Disaster Management Research, Training, and Discovery | 174 |
| <i>Irma Becerra-Fernandez and Greg Madey</i> | |
| Fingerprint Recognition..... | 180 |
| <i>Gualberto Aguilar, Gabriel Sánchez, Karina Toscano, Moisés Salinas, Mariko Nakano, and Hector Perez</i> | |
| A Model Supporting Business Continuity Auditing and Planning in Information Systems..... | 186 |
| <i>Emmanuele Zambon, Damiano Bolzoni, Sandro Etalle, and Marco Salvato</i> | |

ICGD&BC 2/TRACK

| | |
|--|-----|
| GPSDTN: Predictive Velocity-Enabled Delay-Tolerant Networks for Arctic Research and Sustainability | 195 |
| <i>R. Beck, K. Hinkel, W. Eisner, L. Liu, Jacob Norda, Ngoc Hoang, Kevin Fall, Jian Li, Moses Garuba, Richard Machinda, Steve Smith, S. Burleigh, L. Torgerson, A. Hooke, Robert Bulger, Glenn Sheehan, Ben Ellis, Robert Durst, Avri Doria, Maria Uden, James Ferl, D. Pleva, W. Ivancic, P. Paulsen, Ward Bathrick, G. Parr, C. Peoples, B. Scotney, A. Moore, Charles Lambert, Steven Groves, Christopher Small, Lawrence Freudinger, Jason LeBrun, Marc Seibert, and Andrew Maffei</i> | |
| Service Supplier Infrastructure for Location-Based M-Commerce | 205 |
| <i>P. D. Mzila, M. O. Adigun, and S. S. Xulu</i> | |
| Ex-RBAC: An Extended Role Based Access Control Model for Location-Aware Mobile Collaboration System | 211 |
| <i>Xiutao Cui, Yuliang Chen, and Junzhong Gu</i> | |
| Mobile Location Using Super-Resolution Algorithms | 217 |
| <i>Raúl O. González-Pacheco and Felipe Catedra</i> | |
| Path Planning and Following Algorithms in an Indoor Navigation Model for Visually Impaired..... | 223 |
| <i>Hua Wu, Alan Marshall, and Wai Yu</i> | |
| Creating a Dynamic Picture of Network Participant Geospatial Information in Complex Terrains | 230 |
| <i>Paul Labbé, Louise Lamont, Ying Ge, and Li Li</i> | |

ICGD&BC 3

| | |
|--|-----|
| Quantifying the Possible Financial Consequences of Failure for Making a Risk Based Decision | 237 |
| <i>Omar Khadeer Hussain, Elizabeth Chang, Farookh Khadeer Hussain, and Tharam S. Dillon</i> | |
| A Model for Credential Based Exception Management in Digital Rights Management Systems | 243 |
| <i>Jean-Henry Morin and Michel Pawlak</i> | |
| State of the Art Review of the Existing Soft Computing Based Approaches to Trust and Reputation Computation | 252 |
| <i>Farookh Khadeer Hussain, Elizabeth Chang, and Omar Khadeer Hussain</i> | |
| State of the Art Review of the Existing PageRank™ Based Algorithms for Trust and Reputation Computation | 256 |
| <i>Farookh Khadeer Hussain, Elizabeth Chang, and Omar Khadeer Hussain</i> | |

Author Index