International Association of Science
and Technology for Development

3rd IASTED International Conference on Communication, Network, and Information Security

CNIS 2006

October 9 - 11, 2006
Cambridge, Massachusetts, USA

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571
www.proceedings.com

ISBN: 978-1-60423-711-5

Some format issues inherent in the e-media version may also appear in this print version.

Proceedings of the Third IASTED International Conference on **Communication, Network, and Information Security**, held October 9 – 11, 2006, Cambridge, Massachusetts, USA.

SPONSORS

The International Association of Science and Technology for Development (IASTED)

- Technical Committee on Communication, Network, and Information Security
- Technical Committee on Networks
- Technical Committee on Information Systems

The International Society for Law and Technology (ISLAT)

EDITOR

S. Rajasekaran – University of Connecticut, USA

KEYNOTE SPEAKER

S.W. Smith – Dartmouth College, USA

TUTORIAL PRESENTERS

J.-H. Cui, Z.J. Shi, and **B. Wang** – University of Connecticut, USA

For each IASTED conference, the following review process is used to ensure the highest level of academic content. Each full manuscript submission is peer reviewed by a minimum of two separate reviewers on the International Program Committee/Additional Reviewers list. The review results are then compiled. If there are conflicting reviews, the paper is sent to a third reviewer.

All photos © Greater Boston Convention & Visitors Bureau.

Copyright © 2006 ACTA Press

ACTA Press
P.O. Box 5124
Anaheim, CA 92814–5124
USA

ACTA Press
B6, Suite #101, 2509 Dieppe Ave SW
Calgary, Alberta T3E 7J9
Canada

ACTA Press
P.O. Box 354
CH–8053 Zurich
Switzerland

Publication Code: 547

International Association of Science and Technology for Development

3rd IASTED International Conference on
Communication, Network, and Information Security
2006

TABLE OF CONTENTS

547-072 ProTemp-Z: An XML based Authorization System with Provisional Authorization and Temporal Certification Support 1
V.V. Singh

547-078 A Robust Image Watermarking Method to Geometric Attacks 7
K. Okada, S. Wada

547-091 Covert Timing Channel Capacity of Rate Monotonic Real-Time Scheduling Algorithm in MLS Systems 13
J. Son, J. Alves-Foss

547-093 Security Analysis of a Large-Scale Voting Scheme 19
S. Eskeland

547-015 A Grey-Level Image Watermarking method based on Block DCT and Statistic Correlation Adjustment 22
C. Obimbo, J. Ni

547-023 An Efficient Authentication Scheme for Contactless Smartcards using Elliptic Curve Ctyptography 28
D.D. Kastanis, I.G. Askoxylakis, A.P. Tragnitis

547-028 Proactive, Content-Aware, Senisitive Data Protection Framework for Enterprises 34
Y. Zhang, R.J. Enbody, J.R. Lloyd

547-063 Slantlet Transform-based Image Fingerprints 41
L.Yu, S. Sun

547-071 A Multi-Bit Watermark Generation Algorithm with Properties of Error Correction 44
B. Salami, C. Obimbo

547-022 Elliptic Curve and Password based Dynamic Key Agreement in Wireless Ad-Hoc Networks 50
I.G. Askoxylakis, D.D. Kastanis, A.P. Traganitis

547-034 A Petri Net Based XML Firewall Security Model for Web Services Invocation 61
M.M. Ayachit, H. Hu

547-042 A Method for Deriving Paths Across a Distributed Web of Trust 68
P. Tipper, C. Edwards

547-043 Designing SSL/TLS Protocol for Resource Constrained Devices 74
A.M. Ali

547-053 Security Framework for Supervisory Control and Data Acquisition, Automation Systems and Networks 81
C. Obombo, F. Haji, L. Lindsay, D. Patel

547-067 Object Authentication in Closed Containers by Ultra-Wideband Multipath Profile Examination: An Application to National Security 87
S. Sobelewski, M. Buehrer

547-089 Self-Organising Quorum Systems for Ad Hoc Networks 93
G. Owen, M. Adda

547-092 Access Control by Secure Multi-Party EPR Decryption in the Medical Scenario 99
S. Eskeland

547-096 The Lightweight Key Management Protocol (LKMP) 104
J. Trostle

547-048 Artificial Immune using Multi-Level Negative Selection Approach to Anomaly Detection 113
A.A.A. Youssif, A.Z. Ghalwash, S.A. Mohamed

547-085 Reinforcement of Privacy in 802.16 MAC Common Part Sublayer using the Principle of Circularity 119
R. Bhakthavathsalam

547-094 An MSLS-EMM for Enforcing Confidentiality in Malicious Environments 126
B. Wang, J. Alves-Foss

547-095 A Classification of Security Patterns for the Transactions Between a Requester, an Intermediary and a Web-Service 132
J. Muñoz Arteaga, R. Mendoza Gonzáles, F.J. Álvarez, M. Vargas Martín

547-097 Security Vulnerability Categories in Major Software Systems 138
O.H. Alhazmi, S.W. Woo, Y.K. Malaiya

547-802 ARP and ICMP Weaknesses: Impact and Network Performance Analysis of a Novel Attack Stategy 144
A. Anand, R. Rishi, M. Kumar

547-803 STRBAC - An Approach Towards Spatio-Temporal Role-based Access Control 150
M. Kumar, R.E. Newman

547-804 Experimental Evaluation of Network Security Through a Hierarchical Quantitative Metrics Model 156
F. El-Hassan, A. Matrawy, N. Seddigh, B. Nandy

547-805 Securing a Linux-based Multi-User Web Server 165
M. Prandini

547-020 Performance Studies of the Server-Side Access Control for SYN-Flooding Distributed Denial of Service Attacks using Real Systems 172
H. Fujinoki, R.K. Boyapati

547-021 A Scalable Approach to IP Anycast Security 179
A. Pathak, D. Sanghi

547-027 An Efficient Hybrid Algorithm for Multidimensional Packet Classification 185
Y. Qi, J. Li

547-030 Introducing Trusted EAP Module for Security Enhancement in WLANs and VPNs 191
P. Urien, M. Dandjinou, M. Badra

547-031 Optimizing Multi-Thread String Matching for Network Processor based Intrusion Management System 199
J. Yu, Q. Huang, Y. Xue

547-033 Dynamically Blocking Access to Web Pages for Spammers' Harvesters 205
T. Eggendorfer, J. Keller

547-045 Design of a Virtual Computer Security Lab 211
J. Keller, R. Naues

547-058 Towards Effective Packet Classification 216
Y. Qi, J. Li

547-059 Access Control Platform for Submitted Jobs in Computational Grid Environment 224
L. Mattes, J.A. Zuffo

Author Index