

*Proceedings*

# IAS 2007

---

---

## Third International Symposium on Information Assurance and Security

29-31 August 2007  
Manchester, United Kingdom

Technically Sponsored by



ICST (International Communication Sciences and Technology Association)



Create-Net (Center of REsearch And Telecommunication Experimentations for  
NETworked communities)



Los Alamitos, California  
Washington • Tokyo



# TABLE OF CONTENTS

## E-COMMERCE SECURITY

<b>Secure M-Commerce Transactions: A Third Party Based Signature Protocol</b> .....	1
<i>L. He, N. Zhang, L. He, I. Rogers</i>	
<b>Secure E-Commerce Protocol for Purchase of e-Goods- Using Smart Card</b> .....	7
<i>S. Devane, M. Chatterjee, D. Phatak</i>	
<b>Certified Email Delivery with Offline TTP</b> .....	13
<i>H. Wang, Y. Ou, J. Ling, L. Liang, X. Xu</i>	
<b>An Effective and Secure Buyer-Seller Watermarking Protocol</b> .....	19
<i>I.M. Ibrahim, S.H.N. El-Din, A.F.A. Hegazy</i>	

## NETWORK SECURITY

<b>Towards an Autonomic Security System for Mobile Ad Hoc Networks</b> .....	25
<i>M. Aljinidi, J. Leneutre</i>	
<b>A Secure Authenticated Key Agreement Protocol For Wireless Security</b> .....	29
<i>P.E. Abi-Char, A. Mhamed, B. El-Hassan</i>	
<b>Hierarchical Multi-Party Key Agreement for Wireless Networks</b> .....	35
<i>S. Eskeland, V. Oleshchuk</i>	
<b>Applying Secure Data Aggregation techniques for a Structure and Density Independent Group Based Key Management Protocol</b> .....	40
<i>K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones</i>	
<b>A Performance Comparison of Wireless Ad Hoc Network Routing Protocols Under Security Attack</b> .....	46
<i>S.M. Bo, H. Xiao, A. Adereti, J.A. Malcolm, B. Christianson</i>	
<b>On Detecting Packets Droppers in MANET: A Novel Low Cost Approach</b> .....	52
<i>T. Fahad, D. Djenouri, R. Askwith</i>	

## CRYPTOGRAPHIC SCHEMES AND APPLICATIONS

<b>Threshold SKI Protocol for ID-based Cryptosystems</b> .....	58
<i>A. Saxena</i>	
<b>Fuzzy Key Extraction from Fingerprint Biometrics based on Dynamic Quantization Mechanism</b> .....	64
<i>T.S. Ong, A.B.J. Teoh</i>	
<b>Low-cost Anonymous Timed-Release Encryption</b> .....	70
<i>D. Hristu-Varsakelis, K. Chalkias, G. Stephanides</i>	
<b>Integrating Multi-Modal Circuit Features Within an Efficient Encryption System</b> .....	76
<i>E. Papoutsis, G. Howells, A. Hopkins, K. McDonald-Maier</i>	
<b>A Secure Authenticated Key Agreement Protocol Based on Elliptic Curve Cryptography</b> .....	82
<i>P.E. Abi-Char, A. Mhamed, B. El-Hassan</i>	

<b>Inclusion of a Montgomery Multiplier Unit into an Embedded Processor’s Datapath to Speed-up Elliptic Curve Cryptography .....</b>	<b>88</b>
<i>S. Bartolini, G. Castagnini, E. Martinelli</i>	

<b>An LSB Data Hiding Technique Using Prime Numbers.....</b>	<b>94</b>
<i>S. Dey, A. Abraham, S. Sanyal</i>	

## **AUTHENTICATION AND ACCESS CONTROL**

<b>Binding Update Authentication Scheme for Mobile IPv6 .....</b>	<b>100</b>
<i>I. Ahmed, U. Tariq, S. Mukhtar, K. Lhee, S.W. Yoo, P. Yanji, M. Hong</i>	

<b>An Authentication Scheme Using Non-Commutative Semigroups.....</b>	<b>106</b>
<i>M.M. Chowdhury</i>	

<b>Function-Based Authorization Constraints Specification and Enforcement .....</b>	<b>110</b>
<i>W. Zhou, C. Meinel</i>	

<b>Separation of Duty in Role-Based Access Control Model through Fuzzy Relations .....</b>	<b>116</b>
<i>H. Takabi, M. Amini, R. Jalili</i>	

<b>Enhancing Role-Based Access Control Model through Fuzzy Relations .....</b>	<b>122</b>
<i>H. Takabi, M. Amini, R. Jalili</i>	

<b>A Theoretical Security Model for Access Control and Security Assurance.....</b>	<b>128</b>
<i>B. Cheng, H. Chen, R. Tseng</i>	

<b>A Purpose-Based Access Control Model .....</b>	<b>134</b>
<i>N. Yang, H. Barringer, N. Zhang</i>	

<b>SARBAC07: A Scoped Administration Model for RBAC with Hybrid Hierarchy.....</b>	<b>140</b>
<i>Y. Zhang, J.B.D. Joshi</i>	

<b>Levels of Authentication Assurance: an Investigation.....</b>	<b>146</b>
<i>A. Nenadic, N. Zhang, L. Yao, T. Morrow</i>	

## **INTRUSION PREVENTION**

<b>Vulnerability Assessment by Learning Attack Specifications in Graphs.....</b>	<b>150</b>
<i>V.N.L. Franqueira, R.H.C. Lopes</i>	

<b>Automatic Patch Generation for Buffer Overflow Attacks.....</b>	<b>154</b>
<i>A. Smirnov, T. Chiueh</i>	

<b>Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks .....</b>	<b>160</b>
<i>M. Sher, T. Magedanz</i>	

<b>Cyber Threat Trend Analysis Model Using HMM .....</b>	<b>166</b>
<i>D.H. Kim, T. Lee, S.D. Jung, H.P. In, H.J. Lee</i>	

<b>DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment .....</b>	<b>172</b>
<i>K. Haslum, A. Abraham, S. Knapkog</i>	

## **INTRUSION DETECTION**

<b>Detection and Honeypot Based Redirection to Counter DDoS Attacks in ISP Domain .....</b>	<b>178</b>
<i>A. Sardana, K. Kumar, R.C. Joshi</i>	
<b>IP Protection: Detecting Email Based Breaches of Confidence .....</b>	<b>184</b>
<i>N. Cooke, L. Gillam, A. Kondoz</i>	
<b>Non-Stationary Markov Models and Anomaly Propagation Analysis in IDS .....</b>	<b>190</b>
<i>A.G. Tokhtabayev, V.A. Skormin</i>	
<b>Building Trustworthy Intrusion Detection through VM Introspection .....</b>	<b>196</b>
<i>F. Baiardi, D. Sgandurra</i>	
<b>Early DoS Attack Detection Using Smoothened Time-Series and Wavelet Analysis .....</b>	<b>202</b>
<i>P. Shinde, S. Guntupalli</i>	
<b>A Security Model for Detecting Suspicious Patterns in Physical Environment.....</b>	<b>208</b>
<i>S. Fong, Z. Yan</i>	
<b>Detection of Web Defacements by means of Genetic Programming.....</b>	<b>214</b>
<i>E. Medvet, C. Fillon, A. Bartoli</i>	

## **SECURITY ANALYSIS**

<b>Team Edit Automata for Testing Security Property.....</b>	<b>220</b>
<i>Z. Yang, A. Hanna, M. Debbabi</i>	
<b>Analysing the Security Threats against Network Convergence Architectures.....</b>	<b>226</b>
<i>P. Argyroudis, R. McAdoo, S. Toner</i>	
<b>Modelling Quality of Protection in Outsourced Business Processes.....</b>	<b>232</b>
<i>F. Massacci, A. Yautsiukhin</i>	
<b>Modeling Security Protocols as Games .....</b>	<b>238</b>
<i>M. Saleh, M. Debbabi</i>	

## **DATA SECURITY AND PRIVACY**

<b>A Secure Storage Service for the gLite Middleware .....</b>	<b>244</b>
<i>D. Scardaci, G. Scuderi</i>	
<b>FPGA/ASIC based Cryptographic Object Store System.....</b>	<b>250</b>
<i>D. Feng, L. Chen, L. Zeng, Z. Niu</i>	
<b>An Architecture for Privacy Preserving Collaborative Filtering on Web Portals .....</b>	<b>256</b>
<i>W. Ahmad, A. Khokhar</i>	
<b>Enforcing Privacy by Means of an Ontology Driven XACML Framework .....</b>	<b>262</b>
<i>D.E.D.I. Abou-Tair, S. Berlik, U. Kelter</i>	
<b>Addressing Privacy Issues in CardSpace .....</b>	<b>268</b>
<i>W.A. Alrodhan, C.J. Mitchell</i>	
<b>Second-LSB-Dependent Robust Watermarking for Relational Database .....</b>	<b>275</b>
<i>X. Xiao, X. Sun, M. Chen</i>	

## **RISK AND TRUST MANAGEMENT**

<b>Operational Risk: Acceptability Criteria</b> .....	281
<i>D.G. Dresner, J.R.G. Wood</i>	
<b>HPRS: A Hybrid P2P Reputation System Using File and Peer Rating</b> .....	287
<i>T. Srinivasan, V. Ramachandran, A. Vedachalam, S.K. Ghosh</i>	
<b>Resource Classification Based Negotiation in Web Services</b> .....	293
<i>D.A. Haidar, N. Cuppens, F. Cuppens, H. Debar</i>	
<b>Managing Behaviour Trust in Grids Using Statistical Methods of Quality Assurance</b> .....	299
<i>E. Papalilo, B. Freisleben</i>	
<b>Dynamic Risk Mitigation in Computing Infrastructures</b> .....	305
<i>R.A. Miura-Ko, N. Bambos</i>	
<b>Risk Management in Coalition Networks</b> .....	309
<i>W. Mees</i>	

## **SECURITY REQUIREMENTS AND POLICIES**

<b>On the Definition and Policies of Confidentiality</b> .....	315
<i>J.H. Hammer, G. Schneider</i>	
<b>Enhanced Availability and Security by Rate Control Using Extended Policy Framework in SELinux</b> .....	321
<i>P. Shinde, P. Sharma, S. Guntupalli</i>	
<b>CCARCH: Architecting Common Criteria Security Requirements</b> .....	327
<i>J. Romero-Mariona, H. Ziv, D.J. Richardson</i>	

## **AGENT AND SYSTEM SECURITY**

<b>Organized Anonymous Agents</b> .....	333
<i>M. Warnier, F. Brazier</i>	
<b>Comparing the Trust and Security Models of Mobile Agents</b> .....	339
<i>M. Fragkakis, N. Alexandris</i>	
<b>Program Fragmentation as a Metamorphic Software Protection</b> .....	345
<i>B.D. Birrer, R.A. Raines, R.O. Baldwin, B.E. Mullins, R.W. Bennington</i>	
<b>Accurate Application-Specific Sandboxing for Win32/Intel Binaries</b> .....	351
<i>W. Li, L. Lam, T. Chiueh</i>	

## **WORKSHOP ON COMPUTATIONAL FORENSICS**

<b>Computational Forensics: Towards Hybrid-Intelligent Crime Investigation</b> .....	357
<i>K. Franke, S.N. Srihari</i>	
<b>Shoeprint Image Retrieval Based on Local Image Features</b> .....	361
<i>H. Su, D. Crookes, A. Bouridane, M. Gueham</i>	
<b>Statistical Disk Cluster Classification for File Carving</b> .....	367
<i>C.J. Veenman</i>	

<b>Application of Language Models to Suspect Prioritisation and Suspect Likelihood in Serial Crimes</b> .....	373
<i>R. Bache, F. Crestani, D. Canter, D. Youngs</i>	
<b>Improving the Efficiency of Digital Forensic Search by Means of the Constrained Edit Distance</b> .....	379
<i>S. Petrovic, K. Franke</i>	
<b>Information-theoretical Comparison of Likelihood Ratio Methods of Forensic Evidence Evaluation</b> .....	385
<i>D. Ramos, J. Gonzalez-Rodriguez, G. Zadora, J. Zieba-Palus, C. Aitken</i>	
<b>Study of Structural Features of Handwritten Grapheme 'th' for Writer Identification</b> .....	391
<i>V. Pervouchine, G. Leedham</i>	
<b>Generative Models for Fingerprint Individuality Using Ridge Types</b> .....	397
<i>G. Fang, S.N. Srihari, H. Srinivasan</i>	
<b>Craniofacial Superimposition in Forensic Identification Using Genetic Algorithms</b> .....	403
<i>L. Ballerini, O. Cordon, J. Santamaria, S. Damas, I. Aleman, M. Botella</i>	
<b>The Influence of Frame Length on Speaker Identification Performance</b> .....	409
<i>D. Impedovo, M. Refice</i>	
<b>On Periodic Properties of Interpolation and Their Application To Image Authentications</b> .....	413
<i>B. Mahdian, S. Saic</i>	

## **WORKSHOP ON DATA HIDING FOR INFORMATION AND MULTIMEDIA SECURITY**

<b>Detection of Hidden Information in Webpages Based on Randomness</b> .....	419
<i>J. Huang, X. Sun, H. Huang, G. Luo</i>	
<b>A Weighted Stego Image Detector for Sequential LSB Replacement</b> .....	425
<i>A.D. Ker</i>	
<b>A Framework for Design and Analysis of Asymmetric Fingerprinting Protocols</b> .....	429
<i>G.S. Poh, K.M. Martin</i>	
<b>An Analysis of Database Watermarking Security</b> .....	434
<i>J. Lafaye</i>	
<b>A New Data Hiding Scheme with Quality Control for Binary Images Using Block Parity</b> .....	440
<i>M. Venkatesan, P.M. Devi, K. Duraiswamy, K. Thiagarajah</i>	
<b>Metrics-based Evaluation of Slicing Obfuscations</b> .....	444
<i>A. Majumdar, S. Drape, C. Thomborson</i>	
<b>Structural Digital Signature and Semi-Fragile Fingerprinting for Image Authentication in Wavelet Domain</b> .....	450
<i>Y. Zhu, C. Li, H. Zhao</i>	
<b>A Novel Anti-collusion Coding Scheme Tailored to Track Linear Collusions</b> .....	456
<i>K. Karthik, D. Hatzinakos</i>	
<b>Research on Steganalysis for Text Steganography Based on Font Format</b> .....	462
<i>L. Xiang, X. Sun, G. Luo, C. Gan</i>	
<b>Protection of Mammograms Using Blind Steganography and Watermarking</b> .....	468
<i>Y. Li, C. Li, C. Wei</i>	

**Author Index**