IAS 2007

**Third International Symposium
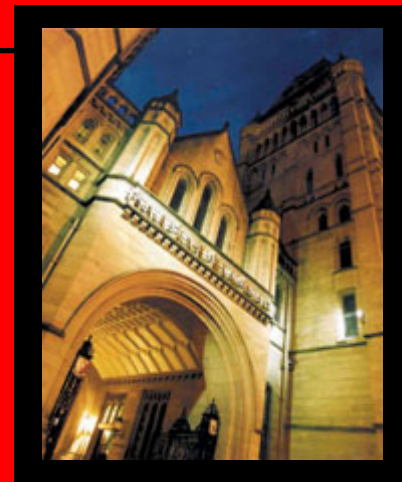on Information Assurance and Security**

**29-31 August 2007
Manchester, United Kingdom**

Sponsored by

ICST (International Communication
Sciences and Technology Association)

Create-Net (Center of REsearch and
Telecommunication Experimentations
for NETworked Communities)

Published by

IEEE
computer society

**Conference
Publishing Services
(CPS)**

Edited by

Ning Zhang,
University of Manchester,
UK

Ajith Abraham,
Norwegian University of
Science and Technology,
Norway

Qi Shi,
Liverpool John Moores
University, UK

Johnson Thomas,
Oklahoma State
University, USA

Conference Information

Third International Symposium on Information Assurance and Security

- ❑ Chairs' Welcome Message
- ❑ IAS 2007 Organisation
- ❑ Keynote Speech
- ❑ Tutorial 1 - Abstract
- ❑ Tutorial 2 - Abstract
- ❑ Title Page (Book version)
- ❑ Copyright Page (Book version)
- ❑ Table of Contents (Book version)
- ❑ Author Index (Book version)
- ❑ Roster Page (Book version)

Sessions

- ❏ E-Commerce Security
- ❏ Network Security
- ❏ Cryptographic Schemes and Applications
- ❏ Authentication and Access Control
- ❏ Intrusion Prevention
- ❏ Intrusion Detection
- ❏ Security Analysis
- ❏ Data Security and Privacy
- ❏ Risk and Trust Management
- ❏ Security Requirements and Policies
- ❏ Agent and System Security
- ❏ Workshop on Computational Forensics
- ❏ Workshop on Data Hiding for Information and Multimedia Security

Papers by Session

E-Commerce Security

❑ Secure M-Commerce Transactions: A Third Party Based Signature Protocol
Lisha He, Ning Zhang, Lirong He, and Ian Rogers

❑ Secure E-Commerce Protocol for Purchase of e-Goods - Using Smart Card
Satish Devane, Madhumita Chatterjee, and Deepak Phatak

❑ Certified Email Delivery with Offline TTP
Hao Wang, Yuyi Ou, Jie Ling, Lu Liang, and Xiang Xu

❑ An Effective and Secure Buyer-Seller Watermarking Protocol
Ibrahim M. Ibrahim, Sherif Hazem Nour El-Din, and Abdel Fatah A. Hegazy

Papers by Session

Network Security

❑ Towards an Autonomic Security System for Mobile Ad Hoc Networks
   Mohamad Aljnidi and Jean Leneutre

❑ A Secure Authenticated Key Agreement Protocol for Wireless Security
   Pierre E. Abi-Char, Abdallah Mhamed, and Bachar El-Hassan

❑ Hierarchical Multi-party Key Agreement for Wireless Networks
   Sigurd Eskeland and Vladimir Oleshchuk

❑ Applying Secure Data Aggregation Techniques for a Structure and Density
   Independent Group Based Key Management Protocol
   Kashif Kifayat, Madjid Merabti, Qi Shi, and David Llewellyn-Jones

❑ A Performance Comparison of Wireless Ad Hoc Network Routing Protocols
   under Security Attack
   Su Mon Bo, Hannan Xiao, Aderemi Adereti, James A. Malcolm, and Bruce Christianson

❑ On Detecting Packets Droppers in MANET: A Novel Low Cost Approach
   Tarag Fahad, Djamel Djenouri, and Robert Askwith

Papers by Session

Cryptographic Schemes and Applications

- Threshold SKI Protocol for ID-Based Cryptosystems
  Ashutosh Saxena

- Fuzzy Key Extraction from Fingerprint Biometrics Based on Dynamic Quantization Mechanism
  Thian Song Ong and Andrew Beng Jin Teoh

- Low-Cost Anonymous Timed-Release Encryption
  D. Hristu-Varsakelis, K. Chalkias, and G. Stephanides

- Integrating Multi-modal Circuit Features within an Efficient Encryption System
  Evangelos Papoutsis, Gareth Howells, Andrew Hopkins, and Klaus McDonald-Maier

- A Secure Authenticated Key Agreement Protocol Based on Elliptic Curve Cryptography
  Pierre E. Abi-Char, Abdallah Mhamed, and Bachar El-Hassan

- Inclusion of a Montgomery Multiplier Unit into an Embedded Processor's Datapath to Speed-Up Elliptic Curve Cryptography
  S. Bartolini, G. Castagnini, and E. Martinelli

- An LSB Data Hiding Technique Using Prime Numbers
  Sandipan Dey, Ajith Abraham, and Sugata Sanyal

Papers by Session

Authentication and Access Control

❑ Binding Update Authentication Scheme for Mobile IPv6
   Irfan Ahmed, Usman Tariq, Shoaib Mukhtar, Kyung-suk Lhee , S.W. Yoo, Piao Yanji, and ManPyo Hong

❑ An Authentication Scheme Using Non-commutative Semigroups
   M. M. Chowdhury

❑ Function-Based Authorization Constraints Specification and Enforcement
   Wei Zhou and Christoph Meinel

❑ Separation of Duty in Role-Based Access Control Model through Fuzzy Relations
   Hassan Takabi, Morteza Amini, and Rasool Jalili

❑ Enhancing Role-Based Access Control Model through Fuzzy Relations
   Hassan Takabi, Morteza Amini, and Rasool Jalili

❑ A Theoretical Security Model for Access Control and Security Assurance
   Bo-Chao Cheng, Huan Chen, and Ryh-Yuh Tseng

❑ A Purpose-Based Access Control Model
   Naikuo Yang, Howard Barringer, and Ning Zhang

❑ SARBAC07: A Scoped Administration Model for RBAC with Hybrid Hierarchy
   Yue Zhang and James B.D. Joshi

Papers by Session

❑ Levels of Authentication Assurance: An Investigation
   Aleksandra Nenadic, Ning Zhang, Li Yao, and Terry Morrow

Papers by Session

Intrusion Prevention

❑ Vulnerability Assessment by Learning Attack Specifications in Graphs
    Virginia N. L. Franqueira, and Raul H. C. Lopes

❑ Automatic Patch Generation for Buffer Overflow Attacks
    Alexey Smirnov and Tzi-cker Chiueh

❑ Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks
    Muhammad Sher and Thomas Magedanz

❑ Cyber Threat Trend Analysis Model Using HMM
    Do Hoon Kim, Taek Lee, Sung-Oh David Jung, Hoh Peter In, and Hee Jo Lee

❑ DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment
    Kjetil Haslum, Ajith Abraham, and Svein Knapskog

Papers by Session

Intrusion Detection

- Detection and Honeypot Based Redirection to Counter DDoS Attacks in ISP Domain
  Anjali Sardana, Krishan Kumar, and R. C. Joshi

- IP Protection: Detecting Email Based Breaches of Confidence
  Neil Cooke, Lee Gillam, and Ahmet Kondoz

- Non-stationary Markov Models and Anomaly Propagation Analysis in IDS
  Arnur G. Tokhtabayev and Victor A. Skormin

- Building Trustworthy Intrusion Detection through VM Introspection
  Fabrizio Baiardi and Daniele Sgandurra

- Early DoS Attack Detection Using Smoothened Time-Series and Wavelet Analysis
  Pravin Shinde and Srinivas Guntupalli

- A Security Model for Detecting Suspicious Patterns in Physical Environment
  Simon Fong and Zhuang Yan

- Detection of Web Defacements by Means of Genetic Programming
  Eric Medvet, Cyril Fillon, and Alberto Bartoli

Papers by Session

Security Analysis

- ❑ Team Edit Automata for Testing Security Property
  Zhenrong Yang, Aiman Hanna, and Mourad Debbabi

- ❑ Analysing the Security Threats against Network Convergence Architectures
  Patroklos Argyroudis, Robert McAdoo, Stephen Toner, Linda Doyle, and Donal O'Mahony

- ❑ Modelling Quality of Protection in Outsourced Business Processes
  Fabio Massacci and Artsiom Yautsiukhin

- ❑ Modeling Security Protocols as Games
  Mohamed Saleh and Mourad Debbabi

Papers by Session

Data Security and Privacy

❑ A Secure Storage Service for the gLite Middleware
  Diego Scardaci and Giordano Scuderi

❑ FPGA/ASIC Based Cryptographic Object Store System
  Dan Feng, Lanxiang Chen, Lingfang Zeng, and Zhongying Niu

❑ An Architecture for Privacy Preserving Collaborative Filtering on Web Portals
  Waseem Ahmad and Ashfaq Khokhar

❑ Enforcing Privacy by Means of an Ontology Driven XACML Framework
  Dhiah el Diehn I. Abou-Tair, Stefan Berlik, and Udo Kelter

❑ Addressing Privacy Issues in CardSpace
  Waleed A. Alrodhan and Chris J. Mitchell

❑ Second-LSB-Dependent Robust Watermarking for Relational Database
  Xiangrong Xiao, Xingming Sun, and Minggang Chen

Papers by Session

Risk and Trust Management

- ❏ Operational Risk: Acceptability Criteria
  Daniel Gideon Dresner and J. Robert (Bob) G. Wood

- ❏ HPRS: A Hybrid P2P Reputation System Using File and Peer Rating
  Srinivasan T., Varun Ramachandran, Arun Vedachalam, and S. K. Ghosh

- ❏ Resource Classification Based Negotiation in Web Services
  Diala Abi Haidar, Nora Cuppens, Frédéric Cuppens, and Hervé Debar

- ❏ Managing Behaviour Trust in Grids Using Statistical Methods of Quality Assurance
  Elvis Papalilo and Bernd Freisleben

- ❏ Dynamic Risk Mitigation in Computing Infrastructures
  R. Ann Miura-Ko and Nicholas Bambos

- ❏ Risk Management in Coalition Networks
  Wim Mees

Papers by Session

Security Requirements and Policies

❑ On the Definition and Policies of Confidentiality
    Johs Hansen Hammer and Gerardo Schneider

❑ Enhanced Availability and Security by Rate Control Using Extended Policy Framework in SELinux
    Pravin Shinde, Priyanka Sharma, and Srinivas Guntupalli

❑ CCARCH: Architecting Common Criteria Security Requirements
    Jose Romero-Mariona, Hadar Ziv, and Debra J. Richardson

Papers by Session

Agent and System Security

❏ Organized Anonymous Agents
   Martijn Warnier and Frances Brazier

❏ Comparing the Trust and Security Models of Mobile Agents
   Michail Fragkakis and Nikolaos Alexandris

❏ Program Fragmentation as a Metamorphic Software Protection
   Bobby D. Birrer, Richard A. Raines, Rusty O. Baldwin, Barry E. Mullins, and Robert W. Bennington

❏ Accurate Application-Specific Sandboxing for Win32/Intel Binaries
   Wei Li, Lap-chung Lam, and Tzi-cker Chiueh

Papers by Session

Workshop on Computational Forensics

- ❑ Computational Forensics: Towards Hybrid-Intelligent Crime Investigation
  Katrin Franke and Sargur N. Srihari

- ❑ Shoeprint Image Retrieval Based on Local Image Features
  H. Su, D. Crookes, A. Bouridane, and M. Gueham

- ❑ Statistical Disk Cluster Classification for File Carving
  Cor J. Veenman

- ❑ Application of Language Models to Suspect Prioritisation and Suspect Likelihood
  in Serial Crimes
  Richard Bache, Fabio Crestani, David Canter, and Donna Youngs

- ❑ Improving the Efficiency of Digital Forensic Search by Means of the Constrained
  Edit Distance
  Slobodan Petrovi and Katrin Franke

- ❑ Information-Theoretical Comparison of Likelihood Ratio Methods of Forensic
  Evidence Evaluation
  Daniel Ramos, Joaquin Gonzalez-Rodriguez, Grzegorz Zadora, Janina Zieba-Palus,
  and Colin Aitken

Papers by Session

❑ Study of Structural Features of Handwritten Grapheme 'th' for Writer Identification
    Vladimir Pervouchine and Graham Leedham

❑ Generative Models for Fingerprint Individuality Using Ridge Types
    Gang Fang, Sargur N. Srihari, and Harish Srinivasan

❑ Craniofacial Superimposition in Forensic Identification Using Genetic Algorithms
    Lucia Ballerini, Oscar Cordon, Sergio Damas, Jose Santamaría, Inmaculada Aleman,
    and Miguel Botella

❑ The Influence of Frame Length on Speaker Identification Performance
    Donato Impedovo and Mario Refice

❑ On Periodic Properties of Interpolation and Their Application to Image Authentication
    Babak Mahdian and Stanislav Saic

Papers by Session

Workshop on Data Hiding for Information and Multimedia Security

❑ Detection of Hidden Information in Webpages Based on Randomness
Junwei Huang, Xingming Sun, Huajun Huang, and Gang Luo

❑ A Weighted Stego Image Detector for Sequential LSB Replacement
Andrew D. Ker

❑ A Framework for Design and Analysis of Asymmetric Fingerprinting Protocols
Geong Sen Poh and Keith M. Martin

❑ An Analysis of Database Watermarking Security
Julien Lafaye

❑ A New Data Hiding Scheme with Quality Control for Binary Images Using Block Parity
M. Venkatesan, P. Meenakshi Devi, K. Duraiswamy, and K. Thiagarajah

❑ Metrics-Based Evaluation of Slicing Obfuscations
Anirban Majumdar, Stephen Drape, and Clark Thomborson

❑ Structural Digital Signature and Semi-fragile Fingerprinting for Image Authentication in Wavelet Domain
Yan Zhu, Chang-Tsun Li, and Hong-Jia Zhao

Papers by Session

❑ A Novel Anti-collusion Coding Scheme Tailored to Track Linear Collusions
  Kannan Karthik and Dimitrios Hatzinakos

❑ Research on Steganalysis for Text Steganography Based on Font Format
  Lingyun Xiang, Xingming Sun, Gang Luo, and Can Gan

❑ Protection of Mammograms Using Blind Steganography and Watermarking
  Yue Li, Chang-Tsun Li, and Chia-Hung Wei

Papers by Author

A

- Abi-Char, Pierre E.
- Abou-Tair, Dhiah el Diehn I.
- Abraham, Ajith
- Adereti, Aderemi
- Ahmad, Waseem
- Ahmed, Irfan
- Aitken, Colin
- Aleman, Inmaculada
- Alexandris, Nikolaos
- Aljnidi, Mohamad
- Alrodhan, Waleed A.
- Amini, Morteza
- Argyroudis, Patroklos
- Askwith, Robert

B

- Bache, Richard
- Baiardi, Fabrizio
- Baldwin, Rusty O.
- Ballerini, Lucia
- Bambos, Nicholas
- Barringer, Howard
- Bartoli, Alberto
- Bartolini, S.
- Bennington, Robert W.
- Berlik, Stefan
- Birrer, Bobby D.
- Bo, Su Mon
- Botella, Miguel
- Bouridane, A.
- Brazier, Frances

Papers by Author

C

- Canter, David
- Castagnini, G.
- Chalkias, K.
- Chatterjee, Madhumita
- Chen, Huan
- Chen, Lanxiang
- Chen, Minggang
- Cheng, Bo-Chao
- Chiueh, Tzi-cker
- Chowdhury, M. M.
- Christianson, Bruce
- Cooke, Neil
- Cordon, Oscar
- Crestani, Fabio
- Crookes, D.

- Cuppens, Frédéric
- Cuppens, Nora

D

- Damas, Sergio
- Debar, Hervé
- Debbabi, Mourad
- Devane, Satish
- Devi, P. Meenakshi
- Dey, Sandipan
- Djenouri, Djamel
- Doyle, Linda
- Drape, Stephen
- Dresner, Daniel Gideon
- Duraiswamy, K.

Papers by Author

E

- ❑ El-Din, Sherif Hazem Nour
- ❑ El-Hassan, Bachar
- ❑ Eskeland, Sigurd

F

- ❑ Fahad, Tarag
- ❑ Fang, Gang
- ❑ Feng, Dan
- ❑ Fillon, Cyril
- ❑ Fong, Simon
- ❑ Fragkakis, Michail
- ❑ Franke, Katrin
- ❑ Franqueira, Virginia N. L.
- ❑ Freisleben, Bernd

G

- ❑ Gan, Can
- ❑ Ghosh, S. K.
- ❑ Gillam, Lee
- ❑ Gonzalez-Rodriguez, Joaquin
- ❑ Gueham, M.
- ❑ Guntupalli, Srinivas

H

- ❑ Haidar, Diala Abi
- ❑ Hammer, Johs Hansen
- ❑ Hanna, Aiman
- ❑ Haslum, Kjetil
- ❑ Hatzinakos, Dimitrios
- ❑ He, Lirong
- ❑ He, Lisha

Papers by Author

- Hegazy, Abdel Fatah A.
- Hong, ManPyo
- Hopkins, Andrew
- Howells, Gareth
- Hristu-Varsakelis, D.
- Huang, Huajun
- Huang, Junwei

I

- Ibrahim, Ibrahim M.
- Impedovo, Donato
- In, Hoh Peter

J

- Jalili, Rasool
- Joshi, James B.D.
- Joshi, R. C.

- Jung, Sung-Oh David

K

- Karthik, Kannan
- Kelter, Udo
- Ker, Andrew D.
- Khokhar, Ashfaq
- Kifayat, Kashif
- Kim, Do Hoon
- Knapskog, Svein
- Kondoz, Ahmet
- Kumar, Krishan

L

- Lafaye, Julien
- Lam, Lap-chung
- Lee, Hee Jo

Papers by Author

- Lee, Taek
- Leedham, Graham
- Leneutre, Jean
- Lhee, Kyung-suk
- Li, Chang-Tsun
- Li, Wei
- Li, Yue
- Liang, Lu
- Ling, Jie
- Llewellyn-Jones, David
- Lopes, Raul H. C.
- Luo, Gang

M

- Magedanz, Thomas
- Mahdian, Babak
- Majumdar, Anirban

- Malcolm, James A.
- Martin, Keith M.
- Martinelli, E.
- Massacci, Fabio
- McAdoo, Robert
- McDonald-Maier, Klaus
- Medvet, Eric
- Mees, Wim
- Meinel, Christoph
- Merabti, Madjid
- Mhamed, Abdallah
- Mitchell, Chris J.
- Miura-Ko, R. Ann
- Morrow, Terry
- Mukhtar, Shoaib
- Mullins, Barry E.

Papers by Author

N

- ❑ Nenadic, Aleksandra
- ❑ Niu, Zhongying

O

- ❑ O'Mahony, Donal
- ❑ Oleshchuk, Vladimir
- ❑ Ong, Thian Song
- ❑ Ou, Yuyi

P

- ❑ Papalilo, Elvis
- ❑ Papoutsis, Evangelos
- ❑ Pervouchine, Vladimir
- ❑ Petrovi, Slobodan
- ❑ Phatak, Deepak

- ❑ Poh, Geong Sen

R

- ❑ Raines, Richard A.
- ❑ Ramachandran, Varun
- ❑ Ramos, Daniel
- ❑ Refice, Mario
- ❑ Richardson, Debra J.
- ❑ Rogers, Ian
- ❑ Romero-Mariona, Jose

S

- ❑ Saic, Stanislav
- ❑ Saleh, Mohamed
- ❑ Santamaría, Jose
- ❑ Sanyal, Sugata
- ❑ Sardana, Anjali

Papers by Author

- Saxena, Ashutosh
- Scardaci, Diego
- Schneider, Gerardo
- Scuderi, Giordano
- Sgandurra, Daniele
- Sharma, Priyanka
- Sher, Muhammad
- Shi, Qi
- Shinde, Pravin
- Skormin, Victor A.
- Smirnov, Alexey
- Srihari, Sargur N.
- Srinivasan, Harish
- Stephanides, G.
- Su, H.
- Sun, Xingming

T

- T., Srinivasan
- Takabi, Hassan
- Tariq, Usman
- Teoh, Andrew Beng Jin
- Thiagarajah, K.
- Thomborson, Clark
- Tokhtabayev, Arnur G.
- Toner, Stephen
- Tseng, Ryh-Yuh

V

- Vedachalam, Arun
- Veenman, Cor J.
- Venkatesan, M.

Papers by Author

W

- Wang, Hao
- Warnier, Martijn
- Wei, Chia-Hung
- Wood, J. Robert (Bob) G.

X

- Xiang, Lingyun
- Xiao, Hannan
- Xiao, Xiangrong
- Xu, Xiang

Y

- Yan, Zhuang
- Yang, Naikuo
- Yang, Zhenrong
- Yanji, Piao
- Yao, Li
- Yautsiukhin, Artsiom
- Yoo, S.W.
- Youngs, Donna

Z

- Zadora, Grzegorz
- Zeng, Lingfang
- Zhang, Ning
- Zhang, Yue
- Zhao, Hong-Jia
- Zhou, Wei
- Zhu, Yan
- Zieba-Palus, Janina
- Ziv, Hadar

Papers by Author

Abi-Char, Pierre E.

- ❑ A Secure Authenticated Key Agreement Protocol for Wireless Security
- ❑ A Secure Authenticated Key Agreement Protocol Based on Elliptic Curve Cryptography

Abou-Tair, Dhiah el Diehn I.

- ❑ Enforcing Privacy by Means of an Ontology Driven XACML Framework

Abraham, Ajith

- ❑ An LSB Data Hiding Technique Using Prime Numbers
- ❑ DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment

Adereti, Aderemi

- ❑ A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack

Papers by Author

Ahmad, Waseem

❑ An Architecture for Privacy Preserving Collaborative Filtering on Web Portals

Ahmed, Irfan

❑ Binding Update Authentication Scheme for Mobile IPv6

Aitken, Colin

❑ Information-Theoretical Comparison of Likelihood Ratio Methods of Forensic Evidence Evaluation

Aleman, Inmaculada

❑ Craniofacial Superimposition in Forensic Identification Using Genetic Algorithms

Alexandris, Nikolaos

❑ Comparing the Trust and Security Models of Mobile Agents

Papers by Author

Aljnidi, Mohamad

❑ Towards an Autonomic Security System for Mobile Ad Hoc Networks

Alrodhan, Waleed A.

❑ Addressing Privacy Issues in CardSpace

Amini, Morteza

❑ Separation of Duty in Role-Based Access Control Model through Fuzzy Relations
❑ Enhancing Role-Based Access Control Model through Fuzzy Relations

Argyroudis, Patroklos

❑ Analysing the Security Threats against Network Convergence Architectures

Askwith, Robert

❑ On Detecting Packets Droppers in MANET: A Novel Low Cost Approach

Papers by Author

Bache, Richard

❑ Application of Language Models to Suspect Prioritisation and Suspect Likelihood in Serial Crimes

Baiardi, Fabrizio

❑ Building Trustworthy Intrusion Detection through VM Introspection

Baldwin, Rusty O.

❑ Program Fragmentation as a Metamorphic Software Protection

Ballerini, Lucia

❑ Craniofacial Superimposition in Forensic Identification Using Genetic Algorithms

Bambos, Nicholas

❑ Dynamic Risk Mitigation in Computing Infrastructures

Papers by Author

Barringer, Howard

❑ A Purpose-Based Access Control Model

Bartoli, Alberto

❑ Detection of Web Defacements by Means of Genetic Programming

Bartolini, S.

❑ Inclusion of a Montgomery Multiplier Unit into an Embedded Processor's Datapath to Speed-Up Elliptic Curve Cryptography

Bennington, Robert W.

❑ Program Fragmentation as a Metamorphic Software Protection

Berlik, Stefan

❑ Enforcing Privacy by Means of an Ontology Driven XACML Framework

Papers by Author

Birrer, Bobby D.

- ❑ Program Fragmentation as a Metamorphic Software Protection

Bo, Su Mon

- ❑ A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack

Botella, Miguel

- ❑ Craniofacial Superimposition in Forensic Identification Using Genetic Algorithms

Bouridane, A.

- ❑ Shoeprint Image Retrieval Based on Local Image Features

Brazier, Frances

- ❑ Organized Anonymous Agents

Papers by Author

Canter, David

❑ Application of Language Models to Suspect Prioritisation and Suspect Likelihood in Serial Crimes

Castagnini, G.

❑ Inclusion of a Montgomery Multiplier Unit into an Embedded Processor's Datapath to Speed-Up Elliptic Curve Cryptography

Chalkias, K.

❑ Low-Cost Anonymous Timed-Release Encryption

Chatterjee, Madhumita

❑ Secure E-Commerce Protocol for Purchase of e-Goods - Using Smart Card

Papers by Author

Chen, Huan

❑ A Theoretical Security Model for Access Control and Security Assurance

Chen, Lanxiang

❑ FPGA/ASIC Based Cryptographic Object Store System

Chen, Minggang

❑ Second-LSB-Dependent Robust Watermarking for Relational Database

Cheng, Bo-Chao

❑ A Theoretical Security Model for Access Control and Security Assurance

Chiueh, Tzi-cker

❑ Automatic Patch Generation for Buffer Overflow Attacks
❑ Accurate Application-Specific Sandboxing for Win32/Intel Binaries

Papers by Author

Chowdhury, M. M.

❑ An Authentication Scheme Using Non-commutative Semigroups

Christianson, Bruce

❑ A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack

Cooke, Neil

❑ IP Protection: Detecting Email Based Breaches of Confidence

Cordon, Oscar

❑ Craniofacial Superimposition in Forensic Identification Using Genetic Algorithms

Crestani, Fabio

❑ Application of Language Models to Suspect Prioritisation and Suspect Likelihood in Serial Crimes

Papers by Author

Crookes, D.

❑ Shoeprint Image Retrieval Based on Local Image Features

Cuppens, Frédéric

❑ Resource Classification Based Negotiation in Web Services

Cuppens, Nora

❑ Resource Classification Based Negotiation in Web Services

Damas, Sergio

❑ Craniofacial Superimposition in Forensic Identification Using Genetic Algorithms

Debar, Hervé

❑ Resource Classification Based Negotiation in Web Services

Papers by Author

Debbabi, Mourad

- ❑ Team Edit Automata for Testing Security Property
- ❑ Modeling Security Protocols as Games

Devane, Satish

- ❑ Secure E-Commerce Protocol for Purchase of e-Goods - Using Smart Card

Devi, P. Meenakshi

- ❑ A New Data Hiding Scheme with Quality Control for Binary Images Using Block Parity

Dey, Sandipan

- ❑ An LSB Data Hiding Technique Using Prime Numbers

Papers by Author

Djenouri, Djamel

❑ On Detecting Packets Droppers in MANET: A Novel Low Cost Approach

Doyle, Linda

❑ Analysing the Security Threats against Network Convergence Architectures

Drape, Stephen

❑ Metrics-Based Evaluation of Slicing Obfuscations

Dresner, Daniel Gideon

❑ Operational Risk: Acceptability Criteria

Duraiswamy, K.

❑ A New Data Hiding Scheme with Quality Control for Binary Images Using Block Parity

Papers by Author

El-Din, Sherif Hazem Nour

- ❑ An Effective and Secure Buyer-Seller Watermarking Protocol

El-Hassan, Bachar

- ❑ A Secure Authenticated Key Agreement Protocol for Wireless Security
- ❑ A Secure Authenticated Key Agreement Protocol Based on Elliptic Curve Cryptography

Eskeland, Sigurd

- ❑ Hierarchical Multi-party Key Agreement for Wireless Networks

Fahad, Tarag

- ❑ On Detecting Packets Droppers in MANET: A Novel Low Cost Approach

Papers by Author

Fang, Gang

❑ Generative Models for Fingerprint Individuality Using Ridge Types

Feng, Dan

❑ FPGA/ASIC Based Cryptographic Object Store System

Fillon, Cyril

❑ Detection of Web Defacements by Means of Genetic Programming

Fong, Simon

❑ A Security Model for Detecting Suspicious Patterns in Physical Environment

Fragkakis, Michail

❑ Comparing the Trust and Security Models of Mobile Agents

Papers by Author

Franke, Katrin

- ❑ Computational Forensics: Towards Hybrid-Intelligent Crime Investigation
- ❑ Improving the Efficiency of Digital Forensic Search by Means of the Constrained Edit Distance

Franqueira, Virginia N. L.

- ❑ Vulnerability Assessment by Learning Attack Specifications in Graphs

Freisleben, Bernd

- ❑ Managing Behaviour Trust in Grids Using Statistical Methods of Quality Assurance

Gan, Can

- ❑ Research on Steganalysis for Text Steganography Based on Font Format

Papers by Author

Ghosh, S. K.

- ❑ HPRS: A Hybrid P2P Reputation System Using File and Peer Rating

Gillam, Lee

- ❑ IP Protection: Detecting Email Based Breaches of Confidence

Gonzalez-Rodriguez, Joaquin

- ❑ Information-Theoretical Comparison of Likelihood Ratio Methods of Forensic Evidence Evaluation

Gueham, M.

- ❑ Shoeprint Image Retrieval Based on Local Image Features

Guntupalli, Srinivas

- ❑ Early DoS Attack Detection Using Smoothened Time-Series and Wavelet Analysis

Papers by Author

- ❏ Enhanced Availability and Security by Rate Control Using Extended Policy Framework in SELinux

Haidar, Diala Abi

- ❏ Resource Classification Based Negotiation in Web Services

Hammer, Johs Hansen

- ❏ On the Definition and Policies of Confidentiality

Hanna, Aiman

- ❏ Team Edit Automata for Testing Security Property

Haslum, Kjetil

- ❏ DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment

Papers by Author

Hatzinakos, Dimitrios

❑ A Novel Anti-collusion Coding Scheme Tailored to Track Linear Collusions

He, Lirong

❑ Secure M-Commerce Transactions: A Third Party Based Signature Protocol

He, Lisha

❑ Secure M-Commerce Transactions: A Third Party Based Signature Protocol

Hegazy, Abdel Fatah A.

❑ An Effective and Secure Buyer-Seller Watermarking Protocol

Hong, ManPyo

❑ Binding Update Authentication Scheme for Mobile IPv6

Papers by Author

Hopkins, Andrew

❑ Integrating Multi-modal Circuit Features within an Efficient Encryption System

Howells, Gareth

❑ Integrating Multi-modal Circuit Features within an Efficient Encryption System

Hristu-Varsakelis, D.

❑ Low-Cost Anonymous Timed-Release Encryption

Huang, Huajun

❑ Detection of Hidden Information in Webpages Based on Randomness

Huang, Junwei

❑ Detection of Hidden Information in Webpages Based on Randomness

Papers by Author

Ibrahim, Ibrahim M.

❑ An Effective and Secure Buyer-Seller Watermarking Protocol

Impedovo, Donato

❑ The Influence of Frame Length on Speaker Identification Performance

In, Hoh Peter

❑ Cyber Threat Trend Analysis Model Using HMM

Jalili, Rasool

❑ Separation of Duty in Role-Based Access Control Model through Fuzzy Relations
❑ Enhancing Role-Based Access Control Model through Fuzzy Relations

Joshi, James B.D.

❑ SARBAC07: A Scoped Administration Model for RBAC with Hybrid Hierarchy

Papers by Author

Joshi, R. C.

❑ Detection and Honeypot Based Redirection to Counter DDoS Attacks in ISP Domain

Jung, Sung-Oh David

❑ Cyber Threat Trend Analysis Model Using HMM

Karthik, Kannan

❑ A Novel Anti-collusion Coding Scheme Tailored to Track Linear Collusions

Kelter, Udo

❑ Enforcing Privacy by Means of an Ontology Driven XACML Framework

Ker, Andrew D.

❑ A Weighted Stego Image Detector for Sequential LSB Replacement

Papers by Author

Khokhar, Ashfaq

❑ An Architecture for Privacy Preserving Collaborative Filtering on Web Portals

Kifayat, Kashif

❑ Applying Secure Data Aggregation Techniques for a Structure and Density Independent Group Based Key Management Protocol

Kim, Do Hoon

❑ Cyber Threat Trend Analysis Model Using HMM

Knapskog, Svein

❑ DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment

Papers by Author

Kondoz, Ahmet

❑ IP Protection: Detecting Email Based Breaches of Confidence

Kumar, Krishan

❑ Detection and Honeypot Based Redirection to Counter DDoS Attacks in ISP Domain

Lafaye, Julien

❑ An Analysis of Database Watermarking Security

Lam, Lap-chung

❑ Accurate Application-Specific Sandboxing for Win32/Intel Binaries

Lee, Hee Jo

❑ Cyber Threat Trend Analysis Model Using HMM

Papers by Author

Lee, Taek

❑ Cyber Threat Trend Analysis Model Using HMM

Leedham, Graham

❑ Study of Structural Features of Handwritten Grapheme 'th' for Writer Identification

Leneutre, Jean

❑ Towards an Autonomic Security System for Mobile Ad Hoc Networks

Lhee, Kyung-suk

❑ Binding Update Authentication Scheme for Mobile IPv6

Li, Chang-Tsun

❑ Structural Digital Signature and Semi-fragile Fingerprinting for Image Authentication in Wavelet Domain

❑ Protection of Mammograms Using Blind Steganography and Watermarking

Papers by Author

Li, Wei

❑ Accurate Application-Specific Sandboxing for Win32/Intel Binaries

Li, Yue

❑ Protection of Mammograms Using Blind Steganography and Watermarking

Liang, Lu

❑ Certified Email Delivery with Offline TTP

Ling, Jie

❑ Certified Email Delivery with Offline TTP

Llewellyn-Jones, David

❑ Applying Secure Data Aggregation Techniques for a Structure and Density Independent Group Based Key Management Protocol

Papers by Author

Lopes, Raul H. C.

❑ Vulnerability Assessment by Learning Attack Specifications in Graphs

Luo, Gang

❑ Detection of Hidden Information in Webpages Based on Randomness

❑ Research on Steganalysis for Text Steganography Based on Font Format

Magedanz, Thomas

❑ Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks

Mahdian, Babak

❑ On Periodic Properties of Interpolation and Their Application to Image Authentication

Papers by Author

Majumdar, Anirban

❑ Metrics-Based Evaluation of Slicing Obfuscations

Malcolm, James A.

❑ A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack

Martin, Keith M.

❑ A Framework for Design and Analysis of Asymmetric Fingerprinting Protocols

Martinelli, E.

❑ Inclusion of a Montgomery Multiplier Unit into an Embedded Processor's Datapath to Speed-Up Elliptic Curve Cryptography

Papers by Author

Massacci, Fabio

❑ Modelling Quality of Protection in Outsourced Business Processes

McAdoo, Robert

❑ Analysing the Security Threats against Network Convergence Architectures

McDonald-Maier, Klaus

❑ Integrating Multi-modal Circuit Features within an Efficient Encryption System

Medvet, Eric

❑ Detection of Web Defacements by Means of Genetic Programming

Mees, Wim

❑ Risk Management in Coalition Networks

Papers by Author

Meinel, Christoph

❑ Function-Based Authorization Constraints Specification and Enforcement

Merabti, Madjid

❑ Applying Secure Data Aggregation Techniques for a Structure and Density Independent Group Based Key Management Protocol

Mhamed, Abdallah

❑ A Secure Authenticated Key Agreement Protocol for Wireless Security

❑ A Secure Authenticated Key Agreement Protocol Based on Elliptic Curve Cryptography

Mitchell, Chris J.

❑ Addressing Privacy Issues in CardSpace

Papers by Author

Miura-Ko, R. Ann

❑ Dynamic Risk Mitigation in Computing Infrastructures

Morrow, Terry

❑ Levels of Authentication Assurance: An Investigation

Mukhtar, Shoaib

❑ Binding Update Authentication Scheme for Mobile IPv6

Mullins, Barry E.

❑ Program Fragmentation as a Metamorphic Software Protection

Nenadic, Aleksandra

❑ Levels of Authentication Assurance: An Investigation

Papers by Author

Niu, Zhongying

❑ FPGA/ASIC Based Cryptographic Object Store System

O'Mahony, Donal

❑ Analysing the Security Threats against Network Convergence Architectures

Oleshchuk, Vladimir

❑ Hierarchical Multi-party Key Agreement for Wireless Networks

Ong, Thian Song

❑ Fuzzy Key Extraction from Fingerprint Biometrics Based on Dynamic Quantization Mechanism

Ou, Yuyi

❑ Certified Email Delivery with Offline TTP

Papers by Author

Papalilo, Elvis

- ❑ Managing Behaviour Trust in Grids Using Statistical Methods of Quality Assurance

Papoutsis, Evangelos

- ❑ Integrating Multi-modal Circuit Features within an Efficient Encryption System

Pervouchine, Vladimir

- ❑ Study of Structural Features of Handwritten Grapheme 'th' for Writer Identification

Petrovi, Slobodan

- ❑ Improving the Efficiency of Digital Forensic Search by Means of the Constrained Edit Distance

Phatak, Deepak

- ❑ Secure E-Commerce Protocol for Purchase of e-Goods - Using Smart Card

Papers by Author

Poh, Geong Sen

❏ A Framework for Design and Analysis of Asymmetric Fingerprinting Protocols

Raines, Richard A.

❏ Program Fragmentation as a Metamorphic Software Protection

Ramachandran, Varun

❏ HPRS: A Hybrid P2P Reputation System Using File and Peer Rating

Ramos, Daniel

❏ Information-Theoretical Comparison of Likelihood Ratio Methods of Forensic Evidence Evaluation

Refice, Mario

❏ The Influence of Frame Length on Speaker Identification Performance

Papers by Author

Richardson, Debra J.

❑ CCARCH: Architecting Common Criteria Security Requirements

Rogers, Ian

❑ Secure M-Commerce Transactions: A Third Party Based Signature Protocol

Romero-Mariona, Jose

❑ CCARCH: Architecting Common Criteria Security Requirements

Saic, Stanislav

❑ On Periodic Properties of Interpolation and Their Application to Image Authentication

Saleh, Mohamed

❑ Modeling Security Protocols as Games

Papers by Author

Santamaría, Jose

- ❑ Craniofacial Superimposition in Forensic Identification Using Genetic Algorithms

Sanyal, Sugata

- ❑ An LSB Data Hiding Technique Using Prime Numbers

Sardana, Anjali

- ❑ Detection and Honeypot Based Redirection to Counter DDoS Attacks in ISP Domain

Saxena, Ashutosh

- ❑ Threshold SKI Protocol for ID-Based Cryptosystems

Scardaci, Diego

- ❑ A Secure Storage Service for the gLite Middleware

Papers by Author

Schneider, Gerardo

❑ On the Definition and Policies of Confidentiality

Scuderi, Giordano

❑ A Secure Storage Service for the gLite Middleware

Sgandurra, Daniele

❑ Building Trustworthy Intrusion Detection through VM Introspection

Sharma, Priyanka

❑ Enhanced Availability and Security by Rate Control Using Extended Policy Framework in SELinux

Sher, Muhammad

❑ Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks

Papers by Author

Shi, Qi

- ❑ Applying Secure Data Aggregation Techniques for a Structure and Density Independent Group Based Key Management Protocol

Shinde, Pravin

- ❑ Early DoS Attack Detection Using Smoothened Time-Series and Wavelet Analysis
- ❑ Enhanced Availability and Security by Rate Control Using Extended Policy Framework in SELinux

Skormin, Victor A.

- ❑ Non-stationary Markov Models and Anomaly Propagation Analysis in IDS

Smirnov, Alexey

- ❑ Automatic Patch Generation for Buffer Overflow Attacks

Papers by Author

Srihari, Sargur N.

- ❑ Computational Forensics: Towards Hybrid-Intelligent Crime Investigation
- ❑ Generative Models for Fingerprint Individuality Using Ridge Types

Srinivasan, Harish

- ❑ Generative Models for Fingerprint Individuality Using Ridge Types

Stephanides, G.

- ❑ Low-Cost Anonymous Timed-Release Encryption

Su, H.

- ❑ Shoeprint Image Retrieval Based on Local Image Features

Sun, Xingming

- ❑ Second-LSB-Dependent Robust Watermarking for Relational Database
- ❑ Detection of Hidden Information in Webpages Based on Randomness

Papers by Author

❑ Research on Steganalysis for Text Steganography Based on Font Format

T., Srinivasan

❑ HPRS: A Hybrid P2P Reputation System Using File and Peer Rating

Takabi, Hassan

❑ Separation of Duty in Role-Based Access Control Model through Fuzzy Relations

❑ Enhancing Role-Based Access Control Model through Fuzzy Relations

Tariq, Usman

❑ Binding Update Authentication Scheme for Mobile IPv6

Teoh, Andrew Beng Jin

❑ Fuzzy Key Extraction from Fingerprint Biometrics Based on Dynamic Quantization Mechanism

Papers by Author

Thiagarajah, K.

❑ A New Data Hiding Scheme with Quality Control for Binary Images Using Block Parity

Thomborson, Clark

❑ Metrics-Based Evaluation of Slicing Obfuscations

Tokhtabayev, Arnur G.

❑ Non-stationary Markov Models and Anomaly Propagation Analysis in IDS

Toner, Stephen

❑ Analysing the Security Threats against Network Convergence Architectures

Tseng, Ryh-Yuh

❑ A Theoretical Security Model for Access Control and Security Assurance

Papers by Author

Vedachalam, Arun

❑ HPRS: A Hybrid P2P Reputation System Using File and Peer Rating

Veenman, Cor J.

❑ Statistical Disk Cluster Classification for File Carving

Venkatesan, M.

❑ A New Data Hiding Scheme with Quality Control for Binary Images Using Block Parity

Wang, Hao

❑ Certified Email Delivery with Offline TTP

Warnier, Martijn

❑ Organized Anonymous Agents

Papers by Author

Wei, Chia-Hung

❑ Protection of Mammograms Using Blind Steganography and Watermarking

Wood, J. Robert (Bob) G.

❑ Operational Risk: Acceptability Criteria

Xiang, Lingyun

❑ Research on Steganalysis for Text Steganography Based on Font Format

Xiao, Hannan

❑ A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack

Xiao, Xiangrong

❑ Second-LSB-Dependent Robust Watermarking for Relational Database

Papers by Author

Xu, Xiang

❑ Certified Email Delivery with Offline TTP

Yan, Zhuang

❑ A Security Model for Detecting Suspicious Patterns in Physical Environment

Yang, Naikuo

❑ A Purpose-Based Access Control Model

Yang, Zhenrong

❑ Team Edit Automata for Testing Security Property

Yanji, Piao

❑ Binding Update Authentication Scheme for Mobile IPv6

Papers by Author

Yao, Li

❑ Levels of Authentication Assurance: An Investigation

Yautsiukhin, Artsiom

❑ Modelling Quality of Protection in Outsourced Business Processes

Yoo, S.W.

❑ Binding Update Authentication Scheme for Mobile IPv6

Youngs, Donna

❑ Application of Language Models to Suspect Prioritisation and Suspect Likelihood in Serial Crimes

Zadora, Grzegorz

❑ Information-Theoretical Comparison of Likelihood Ratio Methods of Forensic Evidence Evaluation

Papers by Author

Zeng, Lingfang

❑ FPGA/ASIC Based Cryptographic Object Store System

Zhang, Ning

❑ Secure M-Commerce Transactions: A Third Party Based Signature Protocol

❑ A Purpose-Based Access Control Model

❑ Levels of Authentication Assurance: An Investigation

Zhang, Yue

❑ SARBAC07: A Scoped Administration Model for RBAC with Hybrid Hierarchy

Zhao, Hong-Jia

❑ Structural Digital Signature and Semi-fragile Fingerprinting for Image Authentication in Wavelet Domain

Papers by Author

Zhou, Wei

❑ Function-Based Authorization Constraints Specification and Enforcement

Zhu, Yan

❑ Structural Digital Signature and Semi-fragile Fingerprinting for Image Authentication in Wavelet Domain

Zieba-Palus, Janina

❑ Information-Theoretical Comparison of Likelihood Ratio Methods of Forensic Evidence Evaluation

Ziv, Hadar

❑ CCARCH: Architecting Common Criteria Security Requirements

Papers by Author

A B C D E F G
H I J K L M N
O P Q R S T U
V W X Y Z