

Communications  
in Computer and Information Science 58

Dominik Ślęzak Tai-hoon Kim  
Wai-Chi Fang Kirk P. Arnett (Eds.)

# Security Technology

International Conference, SecTech 2009  
Held as Part of the Future Generation  
Information Technology Conference, FGIT 2009  
Jeju Island, Korea, December 10-12, 2009  
Proceedings



Springer

**Volume Editors**

Dominik Ślezak

University of Warsaw & Infobright Inc., Poland  
E-mail: slezak@infobright.com

Tai-hoon Kim

Hannam University, Daejeon, South Korea  
E-mail: taihoonn@hnu.kr

Wai-Chi Fang

National Chiao Tung University, Hsinchu, Taiwan  
E-mail: wfang@mail.nctu.edu.tw

Kirk P. Arnett

Mississippi State University, Mississippi State, MS, USA  
E-mail: kpa1@msstate.edu

Library of Congress Control Number: 2009940048

CR Subject Classification (1998): E.3, C.2, D.2, D.4.6, K.6.5, C.2.3

ISSN 1865-0929

ISBN-10 3-642-10846-6 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-10846-4 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

[springer.com](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2009  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 12805136 06/3180 5 4 3 2 1 0

## **Foreword**

As future generation information technology (FGIT) becomes specialized and fragmented, it is easy to lose sight that many topics in FGIT have common threads and, because of this, advances in one discipline may be transmitted to others. Presentation of recent results obtained in different disciplines encourages this interchange for the advancement of FGIT as a whole. Of particular interest are hybrid solutions that combine ideas taken from multiple disciplines in order to achieve something more significant than the sum of the individual parts. Through such hybrid philosophy, a new principle can be discovered, which has the propensity to propagate throughout multi-faceted disciplines.

FGIT 2009 was the first mega-conference that attempted to follow the above idea of hybridization in FGIT in a form of multiple events related to particular disciplines of IT, conducted by separate scientific committees, but coordinated in order to expose the most important contributions. It included the following international conferences: Advanced Software Engineering and Its Applications (ASEA), Bio-Science and Bio-Technology (BSBT), Control and Automation (CA), Database Theory and Application (DTA), Disaster Recovery and Business Continuity (DRBC; published independently), Future Generation Communication and Networking (FGCN) that was combined with Advanced Communication and Networking (ACN), Grid and Distributed Computing (GDC), Multimedia, Computer Graphics and Broadcasting (MulGraB), Security Technology (SecTech), Signal Processing, Image Processing and Pattern Recognition (SIP), and u- and e-Service, Science and Technology (UNESST).

We acknowledge the great effort of all the Chairs and the members of advisory boards and Program Committees of the above-listed events, who selected 28% of over 1,050 submissions, following a rigorous peer-review process. Special thanks go to the following organizations supporting FGIT 2009: ECSIS, Korean Institute of Information Technology, Australian Computer Society, SERSC, Springer LNCS/CCIS, COEIA, ICC Jeju, ISEP/IPP, GECAD, PoDIT, Business Community Partnership, Brno University of Technology, KISA, K-NBTC and National Taipei University of Education.

We are very grateful to the following speakers who accepted our invitation and helped to meet the objectives of FGIT 2009: Ruay-Shiung Chang (National Dong Hwa University, Taiwan), Jack Dongarra (University of Tennessee, USA), Xiaohua (Tony) Hu (Drexel University, USA), Irwin King (Chinese University of Hong Kong, Hong Kong), Carlos Ramos (Polytechnic of Porto, Portugal), Timothy K. Shih (Asia University, Taiwan), Peter M.A. Sloot (University of Amsterdam, The Netherlands), Kyu-Young Whang (KAIST, South Korea), and Stephen S. Yau (Arizona State University, USA).

We would also like to thank Rosslin John Robles, Maricel O. Balitanas, Farkhod Alisherov Alisherovich, and Feruza Sattarova Yusfovna – graduate students of Han-nam University who helped in editing the FGIT 2009 material with a great passion.

October 2009

Young-hoon Lee  
Tai-hoon Kim  
Wai-chi Fang  
Dominik Ślezak

## Preface

We would like to welcome you to the proceedings of the 2009 International Conference on Security Technology (SecTech 2009), which was organized as part of the 2009 International Mega-Conference on Future Generation Information Technology (FGIT 2009), held during December 10–12, 2009, at the International Convention Center Jeju, Jeju Island, South Korea.

SecTech 2009 focused on the various aspects of advances in security technology with computational sciences, mathematics and information technology. It provided a chance for academic and industry professionals to discuss recent progress in the related areas. We expect that the conference and its publications will be a trigger for further related research and technology improvements in this important subject.

We would like to acknowledge the great effort of all the Chairs and members of the Program Committee. Out of 140 submissions to SecTech 2009, we accepted 41 papers to be included in the proceedings and presented during the conference. This gives a roughly 30% acceptance ratio. Four of the papers accepted for SecTech 2009 were published in the special FGIT 2009 volume, LNCS 5899, by Springer. The remaining 37 accepted papers can be found in this CCIS volume.

We would like to express our gratitude to all of the authors of submitted papers and to all of the attendees, for their contributions and participation. We believe in the need for continuing this undertaking in the future.

Once more, we would like to thank all the organizations and individuals who supported FGIT 2009 as a whole and, in particular, helped in the success of SecTech 2009.

October 2009

Dominik Ślęzak  
Tai-hoon Kim  
Wai-chi Fang  
Kirk P. Arnett

# **Organization**

## **Organizing Committee**

General Chair	Wai-chi Fang (National Chiao Tung University, Taiwan)
Program Chairs	Tai-hoon Kim (Hannam University, Korea) Kirk P. Arnett (Mississippi State University, USA)
Advisory Board	Dominik Ślezak (University of Warsaw and Infobright, Poland) Edwin H-M. Sha (University of Texas at Dallas, USA) Justin Zhan (CMU, USA) Kouichi Sakurai (Kyushu University, Japan) Laurence T. Yang (St. Francis Xavier University, Canada) Byeong-Ho Kang (University of Tasmania, Australia)
Publicity Chairs	Antonio Coronato (ICAR-CNR, Italy) Damien Sauveron (Université de Limoges / CNRS, France) Hua Liu (Xerox Corporation, USA) Kevin R.B. Butler (Pennsylvania State University, USA) Guojun Wang (Central South University, China) Tao Jiang (Huazhong University of Science and Technology, China) Gang Wu (UESTC, China) Yoshiaki Hori (Kyushu University, Japan) Muhammad Khurram Khan (King Saud University, Saudi Arabia)
Publication Chair	Yong-ik Yoon (Sookmyung Women's University, Korea)

## **Program Committee**

A. Hamou-Lhadj	Hironori Washizaki	Justin Zhan
ByungRae Cha	Hsiang-Cheh Huang	Lejla Batina
Costas Lambrinoudakis	Hyun-Sung Kim	Luigi Buglione
Dieter Gollmann	J.H. Abbawajy	MalRey Lee
E. Konstantinou	Javier Garcia Villalba	Mario Marques Freire
Eduardo B. Fernandez	Jongmoon Baik	Martin Drahansky
Fangguo Zhang	Jordi Forne	Masahiro Mambo
Filip Orsag	Kouichi Sakurai	N. Jaisankar
Gerald Schaefer	Larbi Esmahi	Nobukazu Yoshioka
Hiroaki Kikuchi	Jungsook Kim	Paolo D'Arco

X      Organization

Petr Hanacek  
Qi Shi  
Raphael C.-W. Phan  
Rhee Kyung-Hyune  
Robert Seacord  
Rolf Oppliger  
Rui Zhang  
Serge Chaumette

Sheng-Wei Chen  
Silvia Abrahao  
Stan Kurkovsky  
Stefan Katzenbeisser  
Stefanos Gritzalis  
Swee-Huay Heng  
Tony Shan  
Wen-Shenq Juang

Willy Susilo  
Yannis Stamatou  
Yi Mu  
Yijun Yu  
Yingjiu Li  
Yong Man Ro  
Young Ik Eom

# Table of Contents

Applications of Reversible Data Hiding Techniques with the Quick Response Codes .....	1
<i>Hsiang-Cheh Huang, Feng-Cheng Chang, and Wai-Chi Fang</i>	
A New Approach in T-FA Authentication with OTP Using Mobile Phone .....	9
<i>Abdulaziz S. Almazyad and Yasir Ahmad</i>	
Correlating Alerts into Compressed Graphs Using an Attribute-Based Method and Time Windows .....	18
<i>Seyed Hossein Ahmadinejad and Saeed Jalili</i>	
A Study on Secure Contents Using in Urban Computing .....	26
<i>Hoon Ko, Jongmyung Choi, and Carlos Ramos</i>	
Shadow Generation Protocol in Linguistic Threshold Schemes .....	35
<i>Marek R. Ogiela and Urszula Ogiela</i>	
Analysis of Handwritten Signature Image .....	43
<i>Debnath Bhattacharyya, Poulami Das,         Samir Kumar Bandyopadhyay, and Tai-hoon Kim</i>	
The Design of Signature Selection for Protecting Illegal Outflow of Sensitive Information in Mobile Device .....	51
<i>Bo-heung Chung, Min-ho Han, and Ki-young Kim</i>	
Hardware Based Data Inspection for USB Data Leakage Prevention ....	57
<i>DongHo Kang, BoHeung Jung, and KiYoung Kim</i>	
Grayscale Image Classification Using Supervised Chromosome Clustering .....	64
<i>Debnath Bhattacharyya, Poulami Das,         Samir Kumar Bandyopadhyay, and Tai-hoon Kim</i>	
Towards the Integration of Security Aspects into System Development Using Collaboration-Oriented Models .....	72
<i>Linda Ariani Gunawan, Peter Herrmann, and         Frank Alexander Kraemer</i>	
Impact of Malicious Node on Broadcast Schemes .....	86
<i>Aneel Rahim and Fahad bin Muyaha</i>	
Hierarchical Identity-Based Identification Schemes .....	93
<i>Ji-Jian Chin, Swee-Huay Heng, and Bok-Min Goi</i>	

The Trend of the Security Research for the Insider Cyber Threat . . . . .	100
<i>Jaeseung Hong, Jongwung Kim, and Jeonghun Cho</i>	
MIMO Wiretap Channel: A Scalar Approach . . . . .	108
<i>Mohammad Rakibul Islam and Jinsang Kim</i>	
Security Testing for Operating System and Its System Calls . . . . .	116
<i>Gaoshou Zhai, Hanhui Niu, Na Yang, Minli Tian,     Chengyu Liu, and Hengsheng Yang</i>	
Efficient Group Signature with Forward Secure Revocation . . . . .	124
<i>Haimin Jin, Duncan S. Wong, and Yinlong Xu</i>	
Detecting Distributed Denial of Service Attack Based on Multi-feature Fusion . . . . .	132
<i>Jieren Cheng, Jianping Yin, Yun Liu, Zhiping Cai, and     Chengkun Wu</i>	
Researching on Cryptographic Algorithm Recognition Based on Static Characteristic-Code . . . . .	140
<i>Tie-Ming Liu, Lie-hui Jiang, Hong-qí He, Ji-zhong Li, and Xian Yu</i>	
Verification of Security-Relevant Behavior Model and Security Policy for Model-Carrying Code . . . . .	148
<i>Yonglong Wei, Xiaojuan Zheng, Jinglei Ren, Xudong Zheng,     Chen Sun, and Zhenhao Li</i>	
Feature Level Fusion of Biometrics Cues: Human Identification with Doddington's Caricature . . . . .	157
<i>Dakshina Ranjan Kisku, Phalguni Gupta, and Jamuna Kanta Sing</i>	
A Study on the Interworking for SIP-Based Secure VoIP Communication with Security Protocols in the Heterogeneous Network . . . . .	165
<i>Seokung Yoon, Hyuncheol Jung, and Kyung-Seok Lee</i>	
DDoS Attack Detection Using Three-State Partition Based on Flow Interaction . . . . .	176
<i>Jieren Cheng, Boyun Zhang, Jianping Yin, Yun Liu, and Zhiping Cai</i>	
A Development of Finite State Machine Create Tool for Cryptography Module Validation . . . . .	185
<i>Jae-goo Jeong, Seung-yong Hur, and Gang-Soo Lee</i>	
A Privacy-Aware System Using Threat-Based Evaluation and Feedback Method in Untrusted Ubiquitous Environments . . . . .	193
<i>Yuan Tian, Biao Song, and Eui-Nam Huh</i>	
Fusion of Multiple Matchers Using SVM for Offline Signature Identification . . . . .	201
<i>Dakshina Ranjan Kisku, Phalguni Gupta, and Jamuna Kanta Sing</i>	

A Two-Factor Mutual Authentication Scheme Using Biometrics and Smart Card . . . . .	209
<i>Sheikh Ziauddin</i>	
Secure Collection Tree Protocol for Tamper-Resistant Wireless Sensors . . . . .	217
<i>Peter Pecho, Jan Nagy, Petr Hanáček, and Martin Drahanský</i>	
Accelerometer Based Digital Video Stabilization for Security Surveillance Systems . . . . .	225
<i>Martin Drahanský, Filip Orság, and Petr Hanáček</i>	
Escrowed Deniable Identification Schemes . . . . .	234
<i>Pairat Thorncharoensri, Qiong Huang, Willy Susilo, Man Ho Au, Yi Mu, and Duncan Wong</i>	
Insights into Malware Detection and Prevention on Mobile Phones . . . . .	242
<i>Qiang Yan, Yingjiu Li, Tieyan Li, and Robert Deng</i>	
Automation of Post-exploitation: Focused on MS-Windows Targets . . . . .	250
<i>Mohammad Tabatabai Irani and Edgar R. Weippl</i>	
Speaker Dependent Frequency Cepstrum Coefficients . . . . .	258
<i>Filip Orság</i>	
Towards the Detection of Encrypted BitTorrent Traffic through Deep Packet Inspection . . . . .	265
<i>David A. Carvalho, Manuela Pereira, and Mário M. Freire</i>	
A Simple Encryption Scheme for Binary Elliptic Curves . . . . .	273
<i>Brian King</i>	
Analysis of Text Complexity in a Crypto System – A Case Study on Telugu . . . . .	281
<i>M.S.V.S. Bhadri Raju, B. Vishnu Vardhan, G.A. Naidu, L. Pratap Reddy, and A. Vinaya Babu</i>	
Symmetric-Key Encryption for Wireless Internet SCADA . . . . .	289
<i>Rosslin John Robles and Min-Kyu Choi</i>	
An Efficient Pre-filtering Mechanism for Parallel Intrusion Detection Based on Many-Core GPU . . . . .	298
<i>Chengkun Wu, Jianping Yin, Zhiping Cai, En Zhu, and Jieren Cheng</i>	
<b>Author Index . . . . .</b>	<b>307</b>