

Tai-hoon Kim Hojjat Adeli Wai-chi Fang
Javier García Villalba Kirk P. Arnett
Muhammad Khurram Khan (Eds.)

Security Technology

International Conference SecTech 2011
Held as Part of the Future Generation
Information Technology Conference, FGIT 2011
in Conjunction with GDC 2011
Jeju Island, Korea, December 8-10, 2011
Proceedings

Volume Editors

Tai-hoon Kim

Hannam University, Daejeon, Korea

E-mail: taihoonn@hannam.ac.kr

Hojjat Adeli

The Ohio State University, Columbus, OH, USA

E-mail: adeli.1@osu.edu

Wai-chi Fang

National Chiao Tung University, Hsinchu, Taiwan, R.O.C.

E-mail: wfang@mail.nctu.edu.tw

Javier García Villalba

Universidad Complutense de Madrid, Spain

E-mail: javiergv@fdi.ucm.es

Kirk P. Arnett

Mississippi State University, Oktibbeha, MS, USA

E-mail: kpal1@msstate.edu

Muhammad Khurram Khan

King Saud University, Riyadh, Saudi Arabia

E-mail: mkhurram@ksu.edu.sa

ISSN 1865-0929

e-ISSN 1865-0937

ISBN 978-3-642-27188-5

e-ISBN 978-3-642-27189-2

DOI 10.1007/978-3-642-27189-2

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011943020

CR Subject Classification (1998): C.2, K.6.5, D.4.6, E.3, J.1, H.4

© Springer-Verlag Berlin Heidelberg 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

Security technology is an area that attracts many professionals from academia and industry for research and development. The goal of the SecTech conference is to bring together researchers from academia and industry as well as practitioners to share ideas, problems and solutions relating to the multifaceted aspects of security technology.

We would like to express our gratitude to all of the authors of submitted papers and to all attendees for their contributions and participation.

We acknowledge the great effort of all the Chairs and the members of Advisory Boards and Program Committees of the above-listed event. Special thanks go to SERSC (Science and Engineering Research Support Society) for supporting this conference.

We are grateful in particular to the speakers who kindly accepted our invitation and, in this way, helped to meet the objectives of the conference.

December 2011

Chairs of SecTech 2011

Preface

We would like to welcome you to the proceedings of the 2011 International Conference on Security Technology (SecTech 2011) – the partnering event of the Third International Mega-Conference on Future-Generation Information Technology (FGIT 2011) held during December 8–10, 2011, at Jeju Grand Hotel, Jeju Island, Korea

SecTech 2011 focused on various aspects of advances in security 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 the SecTech 2011 Chairs, Committees, International Advisory Board, Special Session Organizers, as well as all the organizations and individuals who supported the idea of publishing this volume of proceedings, including the SERSC and Springer.

We are grateful to the following keynote, plenary and tutorial speakers who kindly accepted our invitation: Hsiao-Hwa Chen (National Cheng Kung University, Taiwan), Hamid R. Arabnia (University of Georgia, USA), Sabah Mohammed (Lakehead University, Canada), Ruay-Shiung Chang (National Dong Hwa University, Taiwan), Lei Li (Hosei University, Japan), Tadashi Dohi (Hiroshima University, Japan), Carlos Ramos (Polytechnic of Porto, Portugal), Marcin Szczuka (The University of Warsaw, Poland), Gerald Schaefer (Loughborough University, UK), Jinan Fiaidhi (Lakehead University, Canada) and Peter L. Stanchev (Kettering University, USA), Shusaku Tsumoto (Shimane University, Japan), Jemal H. Abawajy (Deakin University, Australia).

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

Last but not the least, we give special thanks to Ronnie D. Caytiles and Yvette E. Gelogo of the graduate school of Hannam University, who contributed to the editing process of this volume with great passion.

This work was supported by the Korean Federation of Science and Technology Societies Grant funded by the Korean Government.

December 2011

Tai-hoon Kim
Hojjat Adeli
Wai Chi Fang
Javier Garcia Villalba
Kirk P. Arnett
Muhammad Khurram Khan

Organization

General Co-chair

Wai Chi Fang	NASA JPL, USA
--------------	---------------

Program Co-chairs

Javier Garcia Villalba	Complutense University of Madrid, Spain
Kirk P. Arnett	Mississippi State University, USA
Muhammad Khurram Khan	King Saud University, Saudi Arabia
Tai-hoon Kim	GVSA and University of Tasmania, Australia

Publicity Co-chairs

Antonio Coronato	ICAR-CNR, Italy
Damien Sauveron	Université de Limoges/CNRS, France
Hua Liu	Xerox Corporation, USA
Kevin Raymond Boyce 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
Aboul Ella Hassanien	Cairo University, Egypt

Publication Chair

Yong-ik Yoon	Sookmyung Women's University, Korea
--------------	-------------------------------------

International Advisory Board

Dominik Slezak	Inforbright, Poland
Edwin H-M. Sha	University of Texas at Dallas, USA
Justin Zhan	CMU, USA
Kouich Sakurai	Kyushu University, Japan
Laurence T. Yang	St. Francis Xavier University, Canada
Byeong-Ho Kang	University of Tasmania, Australia
Aboul Ella Hassanien	Cairo University, Egypt

Program Committee

Abdelouahed Gherbi	Hsiang-Cheh Huang	Raphael C.-W. Phan
Abdelwahab	Hyun-Sung Kim	Reinhard Schwarz
Hamou-Lhadj	J.H. Abbawajy	Rhee Kyung-Hyune
Ahmet Koltuksuz	Jan de Meer	Robert Seacord
Albert Levi	Javier Garcia Villalba	Rodrigo Mello
Ana Lucila S. Orozco	Jongmoon Baik	Rolf Oppliger
ByungRae Cha	Jordi Forne	Rui Zhang
Chamseddine Talhi	Jungsook Kim	SangUk Shin
Chantana	Justin Zhan	S.K. Barai
Chantrapornchai	Kouichi Sakurai	Serge Chaumette
Chin-Feng Lai	Larbi Esmahi	Sheng-Wei Chen
Christos Kalloniatis	Lejla Batina	Silvia Abrahao
Chun-Ying Huang	Luigi Buglione	Stan Kurkovsky
Costas Lambrinouidakis	Martin Drahansky	Stefanos Gritzalis
Despina Polemi	Martin Drahansky	Sungwoon Lee
Dieter Gollmann	Masahiro Mambo	Swee-Huay Heng
Dimitris Geneiatakis	Michael VanHilst	Tony Shan
E. Konstantinou	Michele Risi	Wen-Shenq Juang
Eduardo B. Fernandez	N. Jaisankar	Willy Susilo
Fangguo Zhang	Nobukazu Yoshioka	Yannis Stamatiou
Feng-Cheng Chang	Panagiotis Nastou	Yi Mu
Filip Orsag	MalRey Lee	Yijun Yu
Georgios Kambourakis	Man Ho Au	Yingjiu Li
Gerald Schaefer	Mario Marques Freire	Yong Man Ro
Han-Chieh Chao	Paolo D'Arco	Yoshiaki Hori
Hiroaki Kikuchi	Paolo Falcarin	Young Ik Eom
Hironori Washizaki	Petr Hanacek	Yueh-Hong Chen
Hongji Yang	Pierre-François Bonnefoi	Yun-Sheng Yen
Howon Kim	Qi Shi	

Special Session Organizers

Namje Park
Hee Joon Cho

Table of Contents

On Fast Private Scalar Product Protocols	1
<i>Ju-Sung Kang and Dowon Hong</i>	
A Survey on Access Control Deployment	11
<i>Vivy Suhendra</i>	
Data Anonymity in Multi-Party Service Model	21
<i>Shinsaku Kiyomoto, Kazuhide Fukushima, and Yutaka Miyake</i>	
A Noise-Tolerant Enhanced Classification Method for Logo Detection and Brand Classification	31
<i>Yu Chen and Vrizlynn L.L. Thing</i>	
A Family Constructions of Odd-Variable Boolean Function with Optimum Algebraic Immunity	43
<i>Yindong Chen</i>	
Design of a Modular Framework for Noisy Logo Classification in Fraud Detection	53
<i>Vrizlynn L.L. Thing, Wee-Yong Lim, Junming Zeng, Darell J.J. Tan, and Yu Chen</i>	
Using Agent in Virtual Machine for Interactive Security Training	65
<i>Yi-Ming Chen, Cheng-En Chuang, Hsu-Che Liu, Cheng-Yi Ni, and Chun-Tang Wang</i>	
Information Technology Security Governance Approach Comparison in E-banking	75
<i>Theodosios Tsiakis, Aristeidis Chatzipoulidis, Theodoros Kargidis, and Athanasios Belidis</i>	
A Fast and Secure One-Way Hash Function	85
<i>Lamiaa M. El Bakrawy, Neveen I. Ghali, Aboul Ella Hassanien, and Tai-hoon Kim</i>	
CLAPTCHA- A Novel Captcha	94
<i>Rahul Saha, G. Geetha, and Gang-soo Lee</i>	

An Approach to Provide Security in Wireless Sensor Network Using Block Mode of Cipher	101
<i>Gulshan Kumar, Mritunjay Rai, and Gang-soo Lee</i>	
Microscopic Analysis of Chips	113
<i>Dominik Malcik and Martin Drahansky</i>	
An ID-Based Broadcast Signcryption Scheme Secure in the Standard Model	123
<i>Bo Zhang</i>	
Robust Audio Watermarking Scheme Based on Short Time Fourier Transformation and Singular Value Decomposition	128
<i>Pranab K. Dhar, Mohammad I. Khan, Sunil Dhar, and Jong-Myon Kim</i>	
A Study on Domain Name System as Lookup Manager for Wireless/Mobile Systems in IPv6 Networks	139
<i>Sungkuk Lee, Taeheon Kang, Rosslin John Robles, Sung-Gyu Kim, and Byungjoo Park</i>	
An Information-Theoretic Privacy Criterion for Query Forgery in Information Retrieval	146
<i>David Rebollo-Monedero, Javier Parra-Arnau, and Jordi Forné</i>	
A Distributed, Parametric Platform for Constructing Secure SBoxes in Block Cipher Designs	155
<i>Panayotis E. Nastou and Yannis C. Stamatiou</i>	
Cryptanalysis of an Enhanced Simple Three-Party Key Exchange Protocol	167
<i>Hae-Jung Kim and Eun-Jun Yoon</i>	
An Effective Distance-Computing Method for Network Anomaly Detection	177
<i>Guo-Hui Zhou</i>	
Formalization and Information-Theoretic Soundness in the Development of Security Architecture for Next Generation Network Protocol - UDT	183
<i>Danilo V. Bernardo and Doan B. Hoang</i>	
Bi-Layer Behavioral-Based Feature Selection Approach for Network Intrusion Classification	195
<i>Heba F. Eid, Mostafa A. Salama, Aboul Ella Hassanien, and Tai-hoon Kim</i>	
A Parameterized Privacy-Aware Pub-sub System in Smart Work	204
<i>Yuan Tian, Biao Song, and Eui-Nam Huh</i>	

A Lightweight Access Log Filter of Windows OS Using Simple Debug Register Manipulation	215
<i>Ruo Ando and Kuniyasu Suzuki</i>	
Diversity-Based Approaches to Software Systems Security	228
<i>Abdelouahed Gherbi and Robert Charpentier</i>	
Author Index	239