

Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering

56

Editorial Board

Ozgur Akan

Middle East Technical University, Ankara, Turkey

Paolo Bellavista

University of Bologna, Italy

Jiannong Cao

Hong Kong Polytechnic University, Hong Kong

Falko Dressler

University of Erlangen, Germany

Domenico Ferrari

Università Cattolica Piacenza, Italy

Mario Gerla

UCLA, USA

Hisashi Kobayashi

Princeton University, USA

Sergio Palazzo

University of Catania, Italy

Sartaj Sahni

University of Florida, USA

Xuemin (Sherman) Shen

University of Waterloo, Canada

Mircea Stan

University of Virginia, USA

Jia Xiaohua

City University of Hong Kong, Hong Kong

Albert Zomaya

University of Sydney, Australia

Geoffrey Coulson

Lancaster University, UK

Xuejia Lai Dawu Gu Bo Jin
Yongquan Wang Hui Li (Eds.)

Forensics in Telecommunications, Information, and Multimedia

Third International ICST Conference,
e-Forensics 2010
Shanghai, China, November 11-12, 2010
Revised Selected Papers

Volume Editors

Xuejia Lai

Dawu Gu

Shanghai Jiao Tong University, Department of Computer
Science and Engineering, 200240 Shanghai, P.R. China

E-mail: lai-xj@cs.sjtu.edu.cn; dwgu@sjtu.edu.cn

Bo Jin

The 3rd Research Institute of Ministry of Public Security
Zhang Jiang, Pu Dong, 210031 Shanghai, P.R. China

E-mail: jinbo@stars.org.cn

Yongquan Wang

East China University of Political Science and Law
Shanghai 201620, P. R. China

E-mail: wangyquan@sina.com

Hui Li

Xidian University Xi'an, Shaanxi 710071, P.R. China

E-mail: xd.lihui@gmail.com

ISSN 1867-8211

ISBN 978-3-642-23601-3

DOI 10.1007/978-3-642-23602-0

e-ISSN 1867-822X

e-ISBN 978-3-642-23602-0

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011935336

CR Subject Classification (1998): C.2, K.6.5, D.4.6, I.5, K.4, K.5

© ICST Institute for Computer Science, Social Informatics and Telecommunications Engineering 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)

Preface

E-Forensics 2010, the Third International ICST Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia, was held in Shanghai, China, November 11-12, 2010. The conference was sponsored by ICST in cooperation with Shanghai Jiao Tong University (SJTU), the Natural Science Foundation of China (NSFC), Science and Technology Commission of Shanghai Municipality, Special Funds for International Academic Conferences of Shanghai Jiao Tong University, the 3rd Research Institute of the Ministry of Public Security, China, East China University of Political Science and Law, China, NetInfo Security Press and Xiamen Meiya Pico Information Co. Ltd.

The aim of E-Forensics conferences is to provide a platform for the exchange of advances in areas involving forensics such as digital evidence handling, data carving, records tracing, device forensics, data tamper identification, mobile device locating, etc. The first E-Forensics conference, E-Forensics 2008, was held in Adelaide, Australia, January 21–22, 2008; the second, E-Forensics 2009, was held in Adelaide, Australia, January 19–21, 2009.

This year, the conference received 42 submissions and the Program Committee selected 32 papers after a thorough reviewing process, appear in this volume, together with 5 papers from the Workshop of E-Forensics Law held during the conference. Selected papers are recommended for publication in the journal *China Communications*.

In addition to the regular papers included in this volume, the conference also featured three keynote speeches: “Intelligent Pattern Recognition and Applications” by Patrick S. P. Wang of Northeastern University, USA, “Review on Status of Digital Forensic in China” by Rongsheng Xu of the Chinese Academy of Sciences, China, and “Interdisciplinary Dialogues and the Evolution of Law to Address Cybercrime Issues in the Exciting Age of Information and Communication Technology” by Pauline C. Reich of Waseda University School of Law, Japan.

The TPC decided to give the Best Paper Award to Xiaodong Lin, Chenxi Zhang, and Theodora Dule for their paper “On Achieving Encrypted File Recovery” and the Best Student Paper Award to Juanru Li, Dawu Gu, Chaoguo Deng, and Yuhao Luo for their paper “Digital Forensic Analysis on Runtime Instruction Flow.”

Here, we want to thank all the people who contributed to this conference. First, all the authors who submitted their work; the TPC members and their external reviewers, the organizing team from the Department of Computer Science and Engineering of Shanghai Jiao Tong University—Zhihua Su, Ning Ding,

Jianjie Zhao, Zhiqiang Liu, Shijin Ge, Haining Lu, Huaihua Gu, Bin Long, Kai Yuan, Ya Liu, Qian Zhang, Bailan Li, Cheng Lu, Yuhao Luo, Yinqi Tang, Ming Sun, Wei Cheng, Xinyuan Deng, Bo Qu, Feifei Liu, and Xiaohui Li—for their great efforts in making the conference run smoothly.

November 2010

Xuejia Lai
Dawu Gu
Bo Jin
Yongquan Wang
Hui Li

Organization

Steering Committee Chair

Imrich Chlamtac

President Create-Net Research Consortium

General Chairs

Dawu Gu

Shanghai Jiao Tong University, China

Hui Li

Xidian University, China

Technical Program Chair

Xuejia Lai

Shanghai Jiao Tong University, China

Technical Program Committee

Xuejia Lai

Shanghai Jiao Tong University, China

Barry Blundell

South Australia Police, Australia

Roberto Caldelli

University of Florence, Italy

Kefei Chen

Shanghai Jiao Tong University, China

Thomas Chen

Swansea University, UK

Liping Ding

Institute of Software, Chinese Academy of
Sciences, China

Jordi Forne

Technical University of Catalonia, Spain

Zeno Geradts

The Netherlands Forensic Institute,
The Netherlands

Pavel Gladyshev

University College Dublin, Ireland

Raymond Hsieh

California University of Pennsylvania, USA

Jiwu Huang

Sun Yat-Sen University, China

Bo Jin

The 3rd Research Institute of the Ministry of
Public Security, China

Tai-hoon

Kim Hannam University, Korea

Richard Leary

Forensic Pathway, UK

Hui Li

Xidian University, China

Xuelong Li

University of London, UK

Jeng-Shyang

Pan National Kaohsiung University of
Applied Sciences, Taiwan

Damien Sauveron

University of Limoges, France

Peter Stephenson

Norwich University, USA

Javier Garcia

Villalba Complutense University of Madrid,
Spain

VIII Organization

Jun Wang	China Information Technology Security Evaluation Center
Yongquan Wang	East China University of Political Science and Law, China
Che-Yen Wen	Central Police University, Taiwan
Svein Y. Willassen	Norwegian University of Science and Technology, Norway
Weiqi Yan	Queen's University Belfast, UK
Jianying Zhou	Institute for Infocomm Research, Singapore
Yanli Ren	Shanghai University, China

Workshop Chair

Bo Jin	The 3rd Research Institute of the Ministry of Public Security, China
Yongquan Wang	East China University of Political Science and Law, China

Publicity Chair

Liping Ding	Institute of Software, Chinese Academy of Sciences, China
Avinash Srinivasan	Bloomsburg University, USA
Jun Han	Fudan University, China

Demo and Exhibit Chairs

Hong Su	NetInfo Security Press, China
---------	-------------------------------

Local Chair

Ning Ding	Shanghai Jiao Tong University, China
-----------	--------------------------------------

Publicity Chair

Yuanyuan Zhang	East China Normal University, China
Jianjie Zhao	Shanghai Jiao Tong University, China

Web Chair

Zhiqiang Liu	Shanghai Jiao Tong University, China
--------------	--------------------------------------

Conference Coordinator

Tarja Ryynanen	ICST
----------------	------

Workshop Chairs

Bo Jin	The 3rd Research Institute of the Ministry of Public Security, China
Yongquan Wang	East China University of Political Science and Law, China

Workshop Program Committee

Anthony Reyes	Access Data Corporation, Polytechnic University, USA
Pauline C. Reich	Waseda University, Japan
Pinxin Liu	Renmin University of China, China
Jiang Du	Chongqing University of Posts and Telecommunications, China
Denis Edgar-Nevill	Canterbury Christ Church University, UK
Yonghao Mai	Hubei University of Police, China
Paul Reedy	Manager Forensic Operations Forensic and Data Centres, Australia
Shaopei Shi	Institute of Forensic Science, Ministry of Justice, China
Man Qi	Canterbury Christ Church University, UK
Xufeng Wang	Hangzhou Police Bureau, China
Lin Mei	The 3rd Research Institute of the Ministry of Public Security, China

Table of Contents

On Achieving Encrypted File Recovery	1
<i>Xiaodong Lin, Chenxi Zhang, and Theodora Dule</i>	
Behavior Clustering for Anomaly Detection	14
<i>Xudong Zhu, Hui Li, and Zhijing Liu</i>	
A Novel Inequality-Based Fragmented File Carving Technique	28
<i>Hwei-Ming Ying and Vrizlynn L.L. Thing</i>	
Using Relationship-Building in Event Profiling for Digital Forensic Investigations	40
<i>Lynn M. Batten and Lei Pan</i>	
A Novel Forensics Analysis Method for Evidence Extraction from Unallocated Space	53
<i>Zhenxing Lei, Theodora Dule, and Xiaodong Lin</i>	
An Efficient Searchable Encryption Scheme and Its Application in Network Forensics	66
<i>Xiaodong Lin, Rongxing Lu, Kevin Foxton, and Xuemin (Sherman) Shen</i>	
Attacks on BitTorrent – An Experimental Study	79
<i>Marti Ksionsk, Ping Ji, and Weifeng Chen</i>	
Network Connections Information Extraction of 64-Bit Windows 7 Memory Images	90
<i>Lianhai Wang, Lijuan Xu, and Shuhui Zhang</i>	
RICB: Integer Overflow Vulnerability Dynamic Analysis via Buffer Overflow	99
<i>Yong Wang, Dawu Gu, Jianping Xu, Mi Wen, and Liwen Deng</i>	
Investigating the Implications of Virtualization for Digital Forensics	110
<i>Zheng Song, Bo Jin, Yinghong Zhu, and Yongqing Sun</i>	
Acquisition of Network Connection Status Information from Physical Memory on Windows Vista Operating System	122
<i>Lijuan Xu, Lianhai Wang, Lei Zhang, and Zhigang Kong</i>	
A Stream Pattern Matching Method for Traffic Analysis	131
<i>Can Mo, Hui Li, and Hui Zhu</i>	

Fast in-Place File Carving for Digital Forensics	141
<i>Xinyan Zha and Sartaj Sahni</i>	
Live Memory Acquisition through FireWire	159
<i>Lei Zhang, Lianhai Wang, Ruichao Zhang, Shuhui Zhang, and Yang Zhou</i>	
Digital Forensic Analysis on Runtime Instruction Flow.....	168
<i>Juanru Li, Dawu Gu, Chaoguo Deng, and Yuhao Luo</i>	
Enhance Information Flow Tracking with Function Recognition	179
<i>Kan Zhou, Shiqiu Huang, Zhengwei Qi, Jian Gu, and Beijun Shen</i>	
A Privilege Separation Method for Security Commercial Transactions...	185
<i>Yasha Chen, Jun Hu, Xinmao Gai, and Yu Sun</i>	
Data Recovery Based on Intelligent Pattern Matching	193
<i>JunKai Yi, Shuo Tang, and Hui Li</i>	
Study on Supervision of Integrity of Chain of Custody in Computer Forensics	200
<i>Yi Wang</i>	
On the Feasibility of Carrying Out Live Real-Time Forensics for Modern Intelligent Vehicles.....	207
<i>Saif Al-Kuwari and Stephen D. Wolthusen</i>	
Research and Review on Computer Forensics	224
<i>Hong Guo, Bo Jin, and Daoli Huang</i>	
Text Content Filtering Based on Chinese Character Reconstruction from Radicals	234
<i>Wenlei He, Gongshen Liu, Jun Luo, and Jiuchuan Lin</i>	
Disguisable Symmetric Encryption Schemes for an Anti-forensics Purpose	241
<i>Ning Ding, Dawu Gu, and Zhiqiang Liu</i>	
Digital Signatures for e-Government – A Long-Term Security Architecture.....	256
<i>Przemysław Błażkiewicz, Przemysław Kubiak, and Mirosław Kutylowski</i>	
SQL Injection Defense Mechanisms for IIS+ASP+MSSQL Web Applications.....	271
<i>Beihua Wu</i>	
On Different Categories of Cybercrime in China	277
<i>Aidong Xu, Yan Gong, Yongquan Wang, and Nayan Ai</i>	

Face and Lip Tracking for Person Identification	282
<i>Ying Zhang</i>	
An Anonymity Scheme Based on Pseudonym in P2P Networks	287
<i>Hao Peng, Songnian Lu, Jianhua Li, Aixin Zhang, and Dandan Zhao</i>	
Research on the Application Security Isolation Model	294
<i>Lei Gong, Yong Zhao, and Jianhua Liao</i>	
Analysis of Telephone Call Detail Records Based on Fuzzy Decision Tree	301
<i>Liping Ding, Jian Gu, Yongji Wang, and Jingzheng Wu</i>	
Author Index	313