Guest Editorial Advances in Digital Forensics for Communications and Networking

Computer and Internet crimes are on the rise due to the fast-paced development of computer and Internet technology. Information security in Internet communications and electronic business is essential, and techniques to combat these crimes are required more and more on a daily basis. Network forensics has been an emerging research area for IT-related professionals, researchers, and practitioners since the turn of the century. Crimes committed using data embedding/mining systems, computer systems, network communications, or system detections pose a great threat to information security. Another area of focus in network forensics is how to collect and analyze digital evidence in an existing communication and network environment.

Digital forensics has many challenges, including effective evidence collection and efficient forensic procedures in data mining for evidence trace, custody of evidence chain, digital evidence management and data/image authentication and forensics, cryptography and cryptanalysis in forensics, and network forensics. The interest in digital forensics in network systems can be seen in industrial and standardization efforts accomplished in recent years, including commercial integrated forensic tools developments, the standardization efforts of text-interface to graphic interface to facilitate evidence mining and speed up investigations, and forensic procedures in communication and network systems. This special issue gives a state-of-the-art overview of problems and solution guidelines emerging in current digital forensic research efforts for communication and network systems. A wide variety of topics are addressed, from the physical views such as forensic developments in computer and communication-link environments, to logical views programming of interface connections and testing of forensic tools; from conceptual views, such as effective management of seized evidence and diverse system operations, to user views - in security issues such as authentications, forensic procedures, and ethical and policy issues related to network forensics.

The goal of this special issue is to report on cutting-edge research achievements covering aspects of the forensics and security areas in communications and networks that are distinctively different from security protocols in computer and network systems in general, including information and communication technologies, law, social sciences and business administration. In response to the call for papers, we received a total of 34 submissions, of which 13 papers were selected for publication.

The first six papers in this issue are related to Forensics and Anti-forensics Technologies.

The paper "Attack Pattern Discovery in Forensic Investigation of Network Attacks" by Zhu presents an iterative algorithm for discovering attack patterns via a feedback mechanism, with the degrees of belief for attack instances propagated to the next iteration to further refine the search. The simulations verify that the algorithm achieves accuracy in the digital forensic task of discovering attack patterns.

In "Joint Forensics-Scheduling Strategy for Delay-Sensitive Multimedia Applications over Heterogeneous Networks," Zhou, Chao, and Vasilakos develop a joint forensics-scheduling scheme, which allocates the available network resources based on the affordable forensics overhead and expected quality of service, adaptively adjusts the scalable media-aware forensics, and schedules the transmissions to meet the applications delay constraints.

In "Live Data Mining Concerning Social Networking Forensics Based on a Facebook Session Through Aggregation of Social Data," Chu, Deng, and Park investigate live data acquisition within the RAM of the desktop PC with emphasis on some distinct strings that could be found in order to reconstruct the previous session in a Facebook platform, which plays an extremely precious role for digital forensics investigators to incubate additional thoughtful decisions concerning the discovery of breadcrumb digital evidence.

In "A Plausibly-Deniable, Practical Trusted Platform Module Based Anti-Forensics Client-Server System," Goh, Leong, and Yeo demonstrate a novel approach of using a TPM-enabled computer in a client-server system to hinder forensic examination. The system allows for data confidentiality, plausible deniability, and hiding of traces that data containing incriminating information was present on the client.

The next paper, "Anti-Forensics with Steganographic Data Embedding in Digital Images" by Sun, Weng, Lee, and Yang proposes an anti-forensic steganography method that can embed and extract messages from images. There are two novel approaches developed: the Highlight of Exploiting Modification Direction (HoEMD) and the Adaptive Exploiting Modification Direction (AdEMD). These achieve high efficiency, high quality and large embedding ratios. The proposed steganography system has a larger embedding capacity and a higher image quality. The effectiveness of the proposed steganography schemes over that of a previous blind steganalyzer is demonstrated using the statistical attack of Chi-square analysis.

Digital Object Identifier 10.1109/JSAC.2011.110801

In "On the Typical Statistic Features for Image Blind Steganalysis," Luo, Liu, Lian, Yang, and Gritzalis study steganalysis techniques in multimedia carriers. Such techniques are used to detect the existence of secret messages embedded in digital media. This paper reviews existing feature computing algorithms, compares the two kinds of features, the PDF moments and the CF moments, by analyzing the change trends of the statistic distribution parameters of various frequency subbands before and after message embedding. This provides a theoretical basis for the steganalysis feature selection and extraction. These theoretical results are further confirmed by experimental results. It is expected to provide valuable information to researchers or engineers working in the field of steganography forensics or steganalysis.

The next five papers are related to Evidence Investigations in Attacks.

In "Blacklisting Recommendation System: Using Spatio-Temporal Patterns to Predict Future Attacks," Soldo, Le, and Markopoulou address the problem of forecasting attack sources based on past attack logs from several contributors. This paper formulates this problem as an implicit recommendation system and proposes a multi-level prediction model to solve it.

The paper "A Novel Probabilistic Matching Algorithm for Multi-Stage Attack Forecasts" by Cheng, Liao, Huang, and Yu proposes Judge Evaluation of Attack intensioN (JEAN), an algorithm that inspects the security alerts in the network and provides a probabilistic approach for the prediction of a multi-stage attack by measuring the difference between the stored and the actual multi-stage attack session graphs (ASG).

In "A Flow Classifier with Tamper-Resistant Features and an Evaluation of Its Portability to New Domains," Zou, Kesidis, and Miller propose a TCP flow classifier that employs neither packet header information that is protocol-specific (including port numbers) nor packet-payload information. Techniques based on the former are readily evadable, while detailed yet scalable inspection of packet payloads is difficult to achieve, may violate privacy laws, and is defeated by data encryption. Besides this, it also investigates and evaluates a hypothesis testing approach to detect port spoofing by exploiting confusion matrix statistics.

The next paper "BrowserGuard: A Behavior-Based Solution to Drive-by-Download Attacks" by Tso, Hsu, Yeh, Wang and Chen presents a runtime, browser-based solution, BrowserGuard, to protect a browser against drive-by-download attacks. BrowserGuard records the download scenario of every file that is loaded into a host through a browser. Then based on the download scenario, BrowserGuard blocks the execution of any file that is loaded into a host without the consent of a browser user.

In the paper "Identifying Wireless Users via Transmitter Imperfections," Polak, Dolatshahi, and Goeckel develop algorithms based on statistical signal processing methods to exploit non-linearities of wireless transmitters for the purpose of user identification in wireless systems. The decision rules are derived and their performance is analyzed. In order to establish the viability of the proposed approach, practical variations of transmitter chain components are analyzed based on simulations, measurements and manufacturers' specifications.

The remaining papers are related to Privacy and Secure Protocols.

In "Location Privacy in Unattended Wireless Sensor Networks upon the Requirement of Data Survivability," Chen and Tsai study the trade-off between the data survival rate and the location privacy of a critical node in an UWSN. Obviously, an increase in the number of data replicas can improve the data survival rate, but could severely degrade the location privacy of a critical node. There are three location estimation algorithms proposed: the coordinate median, average of overlapping area and expectation-maximization approaches. The location estimation performance of the proposed schemes is evaluated and the trade-off between the data survival rate and the location privacy is investigated. According to the simulation results, location privacy degrades severely with an increase in the number of data replicas.

In "Optimistic Fair Exchange with Strong Resolution-Ambiguity," Huang, Mu, Susilo, Wu, and Xiang introduce and define a new property for OFE (Optimistic Fair Exchange): Strong Resolution-Ambiguity. The paper shows that many existing OFE protocols have the new property, but its formal investigation has been missing in those protocols. It turns out that in the certified-key model, an OFE protocol is secure in the multi-user setting if it is secure in the single-user setting and has the property of strong resolution-ambiguity.

ACKNOWLEDGMENT

The Guest Editors would like to thank all the authors who have submitted their papers to this special issue. We are indebted to all the referees for their high-quality and timely expert reviews, without which this special issue could not come to fruition. We would also like to express our great gratitude to Dr. Martha Steenstrup, JSAC Editor-in-Chief, Ms. Laurel Greenidge, JSAC Executive Editor, Prof. Pamela Cosman, JSAC Board Representative, Ms. Sue Lange, Online Production Manager, and other JSAC staff, who have all provided significant support throughout the whole process. We hope the contents of this special issue will receive more attention and inspire the readers to invest more resources in the challenges and open problems of this field.

Shiuh-Jeng Wang, *Lead Guest Editor*
Central Police University, Taiwan
sjwang@mail.cpu.edu.tw
dopwang@gmail.com

Javier Lopez, *Guest Editor*
University of Malaga, Spain
jlm@lcc.uma.es

Hamid R. Arabnia, *Guest Editor*
The University of Georgia, USA
hra@cs.uga.edu

Yi Mu, *Guest Editor*
University of Wollongong, Australia
ymu@uow.edu.au

Binod Vaidya, *Guest Editor*
University of Ottawa, Canada
bnvaidya@gmail.com

Jongsung Kim, *Guest Editor*
Kyungnam University, Korea
jongsung.k@gmail.com

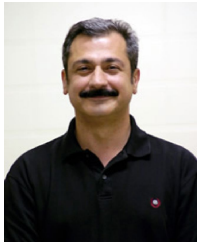
Pamela Cosman, *J-SAC Board Representative*

Shiuh-Jeng Wang was born in Taiwan, 1967. He received the M.S. degree in Applied Mathematics from National Chung-Hsing University, Taichung, Taiwan, in 1991. He received his PhD degree in Electrical Engineering at National Taiwan University, Taipei, Taiwan in 1996. He is currently with Dept. of Information Management at Central Police University, Taoyuan, Taiwan, where he directs the Information Cryptology and Construction Laboratory (ICCL, http://hera.im.cpu.edu.tw). He was a recipient of the 5th Acer Long-Tung Master Thesis Award and the 10th Acer Long-Tung Ph.D Dissertation Award in 1991 and 1996, respectively.

Dr. Wang was a visiting scholar of Computer Science Dept. at Florida State University (FSU), USA in 2002 and 2004. He also was a visiting scholar of Dept. of Computer and Information Science and Engineering at University of Florida (UF) in 2004, 2005, 2010 and 2011. He served the editor-in-chief of the journal of Communications of the CCISA in Taiwan from 2000-2006. He has been elected as the Director of Chinese Cryptology and Information Security Association (CCISA) since 2000. Dr. Wang academically toured the CyLab with School of Computer Science in Carnegie Mellon University, USA, in 2007 for international project collaboration inspection. He is also the authors of eight books (in Chinese versions): Information Security, Cryptography and Network Security, State of the Art on Internet Security and Digital Forensics, Eyes of Privacy Information Security and Computer Forensics, Information Multimedia Security, Computer Forensics and Digital Evidence, Computer Forensics and Security Systems, and Computer and Network Security in Practice, published in 2003, 2004, 2006, 2007, and 2009, respectively.

Prof. Wang has published over 200 papers in referred Journals/Conference proceedings/Technique reports so far. He is a full professor and a member of the IEEE, ACM. His current interests include information security, digital investigation and computer forensics, steganography, cryptography, data construction and engineering. He served a lot of academic and reputable journals in the position of guest-editors. He is currently the corresponding editor- IEEE J-SAC (IEEE Journal on Selected Areas in Communications), at http://www.comsoc.org/livepubs/sac/index.html

Javier Lopez received his M.Sc. and Ph.D. degrees in Computer Science in 1992 and 2000, respectively, from University of Malaga, and from 1991 to 1994 he worked as system analyst in the private sector. He is currently Full Professor, and his activities are mainly focused on network security and critical information infrastructures, leading a number of national and international research projects in those areas, including projects in FP5, FP6 and FP7 European Programmes. Prof. Lopez is the Co-Editor in Chief of International Journal of Information Security (IJIS) and Spanish representative in the IFIP Technical Committee 11 on Security and Protection in Information Systems. Besides, he is member of the Editorial Board of the journals Computers & Security, International Journal of Critical Infrastructures Protection, Computer Networks, and Computer Communications among others.



Hamid R. Arabnia received a Ph.D. degree in Computer Science from the University of Kent (Canterbury, England) in 1987. Dr. Arabnia is currently a Full Professor of Computer Science at University of Georgia (Georgia, USA), where he has been since 1987. His research interests include Parallel and distributed processing techniques and algorithms, interconnection networks, and applications (in particular, in image processing, medical imaging, and other computational intensive problems). Dr. Arabnia is Editor-in-Chief of The Journal of Supercomputing published by Springer and is on the editorial and advisory boards of over 35 other journals and magazines. Dr. Arabnia is the recipient of William F. Rockwell, Jr. Medal for promotion of multi-disciplinary research. In 2000, he was inducted to the World Level of the Hall of Fame for Engineering, Science and Technology (the highest possible level for a living person).

Dr. Arabnia has received a number of prestigious awards; in 2006, he received the Distinguished Service Award "in recognition and appreciation of his contributions to the profession of computer science and his assistance and support to students and scholars from all over the world"; this award was formally presented to him on June 26, 2006 by Professor Barry Vercoe (a founding member of the MIT Media Lab). More recently (October 14, 2007), Dr. Arabnia received an "Outstanding Achievement Award in Recognition of His Leadership and Outstanding Research Contributions to the Field of Supercomputing"; this award was formally presented to him at Harvard University Medical School (signatories: Lawrence O. Hall, President of IEEE/SMC; Zhi-Pei Liang, Vice President of IEEE/EMB; Jack. Y. Yang, General Chair of IEEE BIBE and Harvard University; Mary Qu Yang, Chair of Steering Committee, IEEE BIBE and NIH).

Dr. Arabnia has published extensively in journals and refereed conference proceedings. He has over 300 publications (journals, proceedings, editorship) in his areas of research. He has been a PI/Co-PI on over $8 Million externally funded projects/initiatives. In addition, Dr. Arabnia, during his tenure as Graduate Coordinator/Director of Computer Science (August 2002 – January 2009), secured the largest level of funding in the history of the department for supporting the research and education of graduate students (PhD, MS).

Dr. Arabnia has delivered numerous number of keynote lectures at international conferences; most recently at (since September 2008): The 14th IEEE International Conference on Parallel and Distributed Systems (ICPADS'08, Australia); International Conference on Future Generation Communication and Networking (FGCN 2008 / IEEE CS, Sanya/China); The 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08, Dalian/China), and others. He has also delivered a number of "distinguished lectures" at various universities.

Yi Mu received his PhD from the Australian National University in 1994. He currently is an associate professor, Head of School of Computer Science and Software Engineering and the director of Centre for Computer and Information Security Research, University of Wollongong. His current research interests include network security, computer security, and cryptography. He has published over 250 research papers. Yi Mu is the editor-in-chief of International Journal of Applied Cryptography and serves as editor for nine other international journals. He is a senior member of the IEEE and a member of the IACR.

Binod Vaidya received M.S degree in Radio Communication Engineering from Odessa Electrotechnical Institute of Communications (Odessa National Academy of Telecommunication), Ukraine in 1997 and Ph.D degree in Information and Communication Engineering from Chosun University, Korea in 2007. He was a Post-doctoral Researcher in Chosun University from 09/2007 to 08/2008 and a Research Associate in Gwangju Institute of Science and Technology (GIST) Korea from 09/2008 to 02/2009. From 03/2009 to 02/2010, he was a Researcher in Instituto de Telecomunicaes, Portugal. Since 03/2010, he has been working as a Post-doctoral fellow at the School of Information Technology and Engineering (SITE) of the University of Ottawa, Canada. He has more than 30 publications in international journals and conferences. He has served not only as program chairs in several international conferences and workshops but also as guest editors in several international journals. His current research interests are ubiquitous computing, wireless ad hoc and sensor networks, wireless mesh networks, green networks including smart grid, delay tolerant networks, security, and resilience.

Jongsung Kim obtained his Bachelor and Master degrees in mathematics from Korea university, Korea in 2000 and 2002, respectively. He received double Doctoral degrees on "Combined Differential, Linear and Related-Key Attacks on Block Ciphers and MAC Algorithms", completed in November 2006 and February 2007 at the ESAT/COSIC group of Katholieke Universiteit Leuven and at Engineering in Information Security of Korea University, respectively. He had been a research professor at the Center for Information Security Technologies (CIST), Korea University, Korea, from March 2007 to August 2009. He has been a professor at the division of e-Business, Kyungnam University, Korea, since September 2009. His research interests include symmetric crytosystems, digital forensic, side-channel attacks, ubiquitous computing systems and e-business.