SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2014; **7**:33–35
Published online 8 November 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.646

EDITORIAL

Special Issue on the Design and Engineering of Cryptographic Solutions for Secure Information Systems

This special issue focuses on the effective design and engineering of cryptographic solutions for deployment in secure information systems. Information systems range from those deployed on home computers to state, governmental, and huge enterprise systems using computers connected with local and global networks using wired and wireless and often ad hoc channels of information exchange. In order for the users to have high confidence in those systems for the protection and authentication of stored and/or transmitted data, cryptographic solutions have often been provided as part of security mechanisms. It is essential for such solutions to be designed, implemented, and verified using sound engineering approaches and practices as they must support the core functionality of secure information systems. The designers and engineers need to balance the desired level of security versus financial costs and risks involved in deploying particular solutions in their intended applications. Therefore, the effective design and engineering of cryptographic solutions require a thorough understanding of the requirements of the applications at hand, their constraints and performance characteristics, the capabilities of the hardware and software platforms, and the nature of the network environments.

Submissions for this special issue were open to original, high quality contributions that were not published or currently under review by other archival journals or peer-reviewed conferences with formal proceedings. The authors of the papers presented at *The 3rd International Conference on Security of Information and Networks* (SIN 2010) were especially invited to submit the revised and substantially extended versions of their papers for the special issue. SIN 2010 was organized in technical cooperation with the ACM Special Interest Group on Security, Audit and Control (SIGSAC); it was held on 7–11 September 2010, in Taganrog, Rostov region, Russia. The SIN conference series provides an international forum for presentation of research and applications of security in information and networks, with a special focus on cryptographic solutions in secure information systems, and it was this focus that provided the motivation for the topic of this special issue.

There was an overwhelming interest in the special issue within the security and cryptography communities, and as a result, we received 31 submissions by authors from all over the world. Each submission was sent to three reviewers who were experts in security and cryptography research and closely related areas, with special research interests in cryptographic solutions in both theory and practice. After two rounds of reviewing, nine high quality papers were finally accepted for publication in the special issue, resulting in an acceptance rate of 29%. Many other worthy papers could not be accepted because of the space limitations and the timeliness of the special issue.

The papers cover many important topics in the design and engineering of cryptographic solutions for secure information systems, including hardware design, cryptographic fundamentals, auction design, authentication, routing protocols, protocol verification, detection of collusion attacks, and policy issues. The list of the papers included in the special issue is provided as follows:

1. The paper, *Design and Implementation of a Versatile Cryptographic Unit for RISC Processors* by Kazım Yumbul, Erkay Savaş, Övünç Kocabaş, and Johann Großschädl, discusses the design and implementation of a cryptographic processing unit that can be integrated into any reduced instruction set processor for the safe and efficient execution of cryptographic algorithms.
2. The paper, *Algebraic Construction of Cryptographically Good Binary Linear Transformations* by Bora Aslan and Muharrem Tolga Sakallı, proposes a new algebraic construction method for linear transformations that can be used in block ciphers.
3. The paper, *Efficient Homomorphic Sealed-Bid Auction Free of Bid Validity Check and Equality Test* by Kun Peng, proposes three new homomorphic electronic auction protocols to avoid certain costly operations and improve the efficiency of electronic auctions.
4. The paper, *On Robust Key Agreement Based on Public Key Authentication* by Feng Hao, proposes a new protocol for public key authentication that addresses a number of practical and theoretical flaws of the existing protocols.
5. The paper, *A Secure Many to Many Routing Protocol for Wireless Sensor and Actuator Networks* by Son T. Nguyen, Erdal Çayırcı, and Chunming Rong, proposes a new power aware routing protocol for wireless sensor networks that increases energy efficiency and prolongs network life time.
6. The paper, *A UTP Approach Towards Probabilistic Protocol Verification* by Riccardo Bresciani and Andrew Butterfield, proposes a new probabilistic

approach toward protocol verification, based on an attacker model where cryptographic primitives can be broken probabilistically.

7. The paper, *Exploiting Convergence Characteristics to Tackle Collusion Attacks in OLSR for Security and Communication Networks* by Manoj Singh Gaur, Rajbir Kaur, Lalith P. Suresh, and Vijay Laxmi, describes effective and resource efficient counter-measures for packet dropping attacks such as collusion attacks against optimized link state routing (OLSR) protocol in mobile ad hoc networks.
8. The paper, *Policy Override in Practice: Model, Evaluation, and Decision Support* by Steffen Bartsch, proposes a flexible authorization model, called policy override, that allows end users to override authorization in a secure system in a controlled manner.
9. The paper, *BioPSTM: A Formal Model for Privacy, Security and Trust in Template-Protecting Biometric Authentication* by Alper Kanak and İbrahim Soğukpınar, proposes a new model that formalizes the relationship between trust, privacy, and security and evaluates the model in the context of biometric security technologies.

Many individuals contributed to this special issue. First and foremost, we express our gratitude to Professor Hsiao-Hwa Chen, the Editor-in-Chief of *Security and Communication Networks*, for his continuing support for the special issue. We availed ourselves of his expert opinion at every junction of the whole process. We would also like thank our reviewers who generously donated their time in reading the submissions and providing very detailed and constructive comments for the authors. Their expertise and hard work were instrumental in the decision process. We are indebted to the authors of the 31 submissions who accepted our invitation to submit their best works for the special issue and made such a high quality collection possible in the first place.

We trust that the breadth and diversity of the papers published in this special issue will foster further research on design and engineering of cryptographic solutions in secure information systems ranging from theoretical to practical issues and ultimately to their applications.

Guest Editors

Atilla Elçi
Electrical and Electronics Engineering Department, Aksaray University, Aksaray, Turkey
E-mail: atilla.elci@gmail.com

Josef Pieprzyk
Department of Computing, Macquarie University, Sydney, NSW, Australia

Mehmet A. Orgun
Department of Computing, Macquarie University, Sydney, NSW, Australia

Alexander Chefranov
Computer Engineering Department, Eastern Mediterranean University, Famagusta, Northern Cyprus

AUTHORS' BIOGRAPHIES

Atilla Elçi is full professor and chairman of the Electrical and Electronics Engineering Department, Aksaray University, Aksaray, Turkey since August 2012. He obtained his B.Sc. in Computer/Control Engineering at METU, Ankara, Turkey (1970) and his M.Sc. and Ph.D. in Computer Sciences at Purdue University, West Lafayette, Indiana, USA (in 1973 and 1975, respectively). His research and experience encompass web semantics, agent-based systems, robotics, machine learning, knowledge representation and ontology, information security, and software engineering. He served as full professor and chairman of the Department of the Computer and Educational Technology at Süleyman Demirel University, Isparta, Turkey (May 2011–July 2012). He was full professor of Software Engineering, the founding director of the Graduate School of Science and Technology, and the dean of Engineering Faculty at Toros University, Mersin, Turkey (July 2010–June 2011). He also worked in the Computer Engineering Program of the Middle East Technical University (METU NCC, Spring 2010). He established the Internet Technologies Research Center at the Eastern Mediterranean University (2003–2009). He founded and chaired the Computer Engineering Department at Haliç University, İstanbul, Turkey (2000–2003). He was chief technical advisor in the International Telecommunication Union, Geneva, Switzerland (1985–1997). He was chair and assistant chair of Computer Engineering Department of the METU Ankara, Turkey (1976–1985). He was research assistant at the Purdue University, West Lafayette, Indiana, USA (1974–1975). He has organized or served in the committees of numerous international conferences. He has been organizing IEEE Engineering Semantic Agent Systems Workshops since 2006, Security of Information and Networks Conferences since 2007, and IJRCS Symposiums since 2007. He has published over a hundred journal and conference papers, edited the book Semantic Agent Systems by Springer (2011), Proceedings of SIN 2007, 2009, 2010 by ACM, ESAS 2006–2011 by IEEE CS, and IJRCS 2009. He was COMPSAC 2012's program chair.

Josef Pieprzyk is a professor and chair of Computing at Macquarie University, Sydney, Australia. He received his B.Sc. in Electrical Engineering from Academy of Technology in Bydgoszcz, Poland, his M.Sc. in

Security Comm. Networks 2014; **7**:33–35 © 2012 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

Mathematics from Nicolaus Copernicus University of Torun, Poland, and his Ph.D. degree in Computer Science from the Polish Academy of Sciences, Warsaw, Poland. His main research interest is cryptology and computer security and includes the design and analysis of cryptographic algorithms (such as encryption, hashing, and digital signatures), secure multiparty computations, cryptographic protocols, copyright protection, e-commerce, web security, and cybercrime prevention. He is a member of the editorial boards for International Journal of Information Security, Journal of Mathematical Cryptology, International Journal of Security and Networks, International Journal of Applied Cryptography, and International Journal of Information and Computer Security. He is a member of International Association for Cryptologic Research (IACR). He was instrumental in the creation of both Auscrypt and ACISP conference streams. The Auscrypt stream was later renamed as Asiacrypt. ACISP is the main cryptographic event in Australia and New Zealand. Recently, he was program chair of Asiacrypt 2008 (Melbourne, Australia) and CT-RSA 2010 (San Francisco, USA). He is general chair of ACISP 2010. He has published five books, edited 10 books (conference proceedings published by Springer-Verlag), three book chapters, and more than 200 papers in refereed journals and refereed international conferences.

Mehmet A. Orgun is a professor of Computing at Macquarie University, Sydney, Australia. He received his B.Sc. and M.Sc. degrees in Computer Science and Engineering from Hacettepe University, Ankara, Turkey in 1982 and 1985, respectively, and his Ph.D. degree in Computer Science from the University of Victoria, Canada in 1991. Prior to joining Macquarie University in September 1992, he worked as a post-doctoral fellow at the University of Victoria. He was elevated to the grade of a senior member of IEEE (SMIEEE) in 1996. He researches in the broad area of intelligent systems, with specific research interests in knowledge discovery, trusted systems, multi-agent systems, and industry applications of these research areas. He has served on the program and organizing committees of more than 100 conferences and workshops. More recently, he was the program committee co-chair of The 20th Australian Joint Conference on Artificial Intelligence (AI'07), the program committee co-chair of the 14th Pacific-Rim International Conference on Artificial Intelligence (PRICAI'2010), the conference co-chair of the 2nd and 3rd International Conferences on Security of Information and Networks (SIN 2009 and SIN 2010) and the general chair of the 4th International Conference on Security of Information and Networks (SIN 2011).

Alexander Chefranov holds the degrees of a Ph.D. (Computer Science) and a Doctor of Engineering Sciences. He is currently an associate professor of the Department of Computer Engineering, Eastern Mediterranean University, Famagusta, Northern Cyprus. There he was one of the founders of Internet Technologies Research Center and served as its director in 2008–2009. Prior to joining Eastern Mediterranean University, he was a professor at the Department of Software Engineering at Taganrog State University of Radio-Engineering in Russia. His research interests in information security include symmetric and asymmetric ciphers, authentication and key exchange protocols, and database security. He served as a program committee chair of the 2nd International Conference on Security of Information and Networks (SIN 2009) held in Famagusta in October 2009 and a program committee co-chair of the 3rd International Conference on Security of Information and Networks (SIN 2010) held in Taganrog, Russia in September 2010.