Editorial to the Special Issue on Recent Advances on Trust, Security and Privacy in Computing and Communications

Priyadarsi Nanda[1]*, Deepak Puthal[2] and Saraju P. Mohanty[3]

[1] Faculty of Engineering and IT, University of Technology Sydney, Australia
[2]School of Computing, Newcastle University, UK
[3]Computer Science and Engineering, University of North Texas, USA

*Corresponding Author: Priyadarsi Nanda, Email: Priyadarsi.Nanda@uts.edu.au

1. INTRODUCTION

With the rapid development and increasing complexity of computer systems and communication networks, user requirements for trust, security and privacy are becoming more and more demanding. Therefore, there is a grand challenge that traditional security technologies and measures may not meet user requirements in open, dynamic, heterogeneous, mobile, wireless, and distributed computing environments. Thus, there is a strong need to build systems and networks in which various applications allow users to enjoy more comprehensive services while preserving trust, security and privacy at the same time. As useful and innovative technologies, trusted computing and communications are attracting researchers with more and more attention.

The scope of this special issue is broad and is representative of many important topics involving emerging technologies in the field of Trust, Security, Privacy, Forensics and Data analytics. In addition, the articles selected through this special issue also present strong aspects on theoretical analysis, algorithms, and practical experience in their proposed schemes.

The submissions to the Special Issue were significantly extended research papers from the 16th IEEE International conference on Trust, Security and Privacy in Computing and Communications (Trustcom 2017). This conference brings together researchers and practitioners around the world working on trusted computing and communications, with regard to trust, security, privacy, reliability, dependability, survivability, availability, and fault tolerance aspects of computer systems and networks. All the submissions for this special issue have been reviewed rigorously following the guidelines of Wiley Journal on Concurrency and Computation: Practice and Experience (CCPE). A majority of the reviewers represent expertize in their fields who provided high quality reviews for the manuscripts. The articles selected through a rigorous reviews process for this Special Issue are briefly presented in the rest of this guest editorial.

The guest editors sincerely believe that this special issue on Trust, Security, and Privacy will be a great reading for the contemporary researchers worldwide.

The guest editors would like to thank the editor-in-chief (EiC) Dr. Geoffrey Fox of the Wiley Journal on Concurrency and Computation: Practice and Experience (CCPE) for the opportunity of this special issue. The guest editors are sincerely thankful to the many reviewers around the globe for their timely reviews without which this successful special issue would not have been possible. The guest editors thank the authors for their patience and dedication at all stages of the review process. The guest editors are also thankful to the Wiley production staffs for their help during the production of this special issue.

2. SCANNING THE ISSUE

Fault injection has been increasingly used both to attack software applications and to test system robustness. Detecting fault injection vulnerabilities has been approached with a variety of different but limited methods. Thomas Given-Wilson, et al. [Given-Wilson, 2018] propose extension of a recently published general model checking based process to detect fault injection vulnerabilities in binaries. This new extension makes the general process scalable to real-world implementations. The authors demonstrate their scheme by detecting vulnerabilities in different cryptographic implementations. Fault analysis of AEZ is based on AES using three 128-bit keys. Qahur Al Mahri etal. [Al Mahri, 2018] analysed AEZ 4.2 and investigated the fault issue showing all three 128-bit keys used in AEZ 4.2 can be uniquely retrieved using only three random valued single byte fault injections.

Data publishing may suffer from privacy disclosures, especially, the case in transactional data such as web search and point of sales logs. Current potent privacy preserving mechanisms mainly focus on relational data. Michael Bewong, et al. [Bewong, 2018] propose a new privacy metric for transactional data to prevent inference attacks. Their proposed scheme, Anony ensures that the adversary learns no more about an intended victim than what is publicly available. In order to demonstrate the effectiveness of their scheme, the authors present empirical evaluation on three benchmark datasets.

Mosarrat Jahan, et al. [Jahan, 2018] present selective read/write access to the outsourced data for clients using mobile devices supporting users from multiple domains. The authors use Cipher text-Policy Attribute-based Encryption (CP-ABE) scheme that provide access control on encrypted outsourced data. The proposed scheme provides fine-grained read/write access to the users, accompanied with a lightweight signature scheme and computationally inexpensive user revocation mechanism suitable for resource-constrained mobile devices. Both theoretical analysis of the security protocol and experimental results measured from a real-world testbed strongly validate the proposed scheme.

Yoking-proof scheme is a very useful mechanism in many IoT (Internet of Things) application areas such as health care and supply chain. However existing yoking-proof scheme requires two or more rounds of communication to generate the yoking-proof. Da-Zhi Sun, et al. [Sun, 2018] investigate how to design the one-round yoking-proof scheme with computational efficiency. The scheme is designed with a new timestamp-based scheme for the RFID tag pair. The authors prove the security and privacy of the proposed scheme extending to more than two RFID tags along with one-round of communication to generate the yoking-proof.

While Malware based activities on recent years are slowing down, more and more sophisticated targeting malware have been emerging. These new category of Malwares share little or no common feature with traditional malware. Lansheng Han, et al. [Han, 2018] present classifications of malicious tasks using decidable theory and prove that tasks performed by any software can be recursive and determinable. By establishing a mapping from software to task, they prove their proposition and demonstrate that presence of malwares in software is recursive.

This issue would be incomplete without the article on IoT security. Secured authentication using 6LoWPAN networks is one of the important considerations among various IoT based applications. Existing asymmetric key distribution scheme may not be a perfect choice as recent research shows that Lucky Thirteen attack has compromised Datagram Transport Layer Security (DTLS) with Cipher Block Chaining (CBC) mode for key establishment. Even though EAKES6Lo and S3 K techniques for key establishment follow the symmetric key establishment method, they strongly rely on a remote server and trust anchor.

Annie Gilda Roselin, et al. [Baskaran, 2018] present a Lightweight AUthentication Protocol (LAUP) using symmetric key method with no pre-shared keys between sensors and Edge Router in a 6LoWPAN environment. Their proposed scheme is formally verified using the Scyther security protocol verification tool and the protocol is implemented using COOJA simulator. Finally, the authors develop a Testbed to measure computation time and efficiency of LAUP scheme. The proposed scheme achieves less computational time and low power consumption compared to existing authentication protocols such as the EAKES6Lo and SAKES.

3. REFERENCES

[Al Mahri, 2018]. H. Q. Al Mahri, L. Simpson, H. Bartlett, E Dawson and K. K. H Wong, Fault analysis of AEZ, Concurrency and Computation: Practice and Experience [this issue].

[Baskaran, 2018]. A. G. R. A. Baskaran, P. Nanda, S. Nepal and S. He, Testbed evaluation of Lightweight Authentication Protocol (LAUP) for 6LoWPAN wireless sensor networks, Concurrency and Computation: Practice and Experience [this issue].

[Bewong, 2018]. M. Bewong, J. Liu, L. Liu and K. R. Choo, A relative privacy model for effective privacy preservation in transactional data, Concurrency and Computation: Practice and Experience [this issue].

[Given-Wilson, 2018]. T. Given-Wilson, A. Heuser, N. Jafri and A Legay, An automated and scalable formal process for detecting fault injection vulnerabilities in binaries, Concurrency and Computation: Practice and Experience [this issue].

[Han, 2018]. L. Han, M. Zhou, S. Han, W. Jia, C. Sun and C. Fu, Targeting malware discrimination based on reversed association task, Concurrency and Computation: Practice and Experience [this issue].

[Jahan, 2018]. M. Jahan, S. Seneviratne, P. S. Roy, K. Sakurai, A Seneviratne and S. Jha, Light weight and fine-grained access mechanism for secure access to outsourced data, Concurrency and Computation: Practice and Experience [this issue].

[Sun, 2018]. D. Sun, Z. Zhu, G. Xu and W. Guo, One-round provably secure yoking-proof for RFID applications, Concurrency and Computation: Practice and Experience [this issue].

4. ABOUT THE GUEST EDITORS

Priyadarsi Nanda obtained his PhD in Computing Science from University of Technology Sydney, Australia, Master's degree in Computer and Telecommunication Engineering from University of Wollongong, Australia and Bachelor of Engineering with Distinction in Computer Engineering from Shivaji University, India. He is a Senior Lecturer at the University of Technology Sydney (UTS), Australia with more than 28 years of experience specialising in research and development in Cybersecurity, IoT security, Internet Traffic Engineering, wireless sensor network security and many more related areas. His most significant work has been in the area of Intrusion detection and prevention systems (IDS/IPS) using image processing techniques, Sybil attack detection in IoT based applications, intelligent firewall design. He has authored more than 100 research articles including Transactions in Computers, Transactions in Parallel Processing and Distributed Systems (TPDS), Future Generations of Computer Systems (FGCS) as well as many ERA Tier A/A* conference articles. In 2017, his work in cyber security research has earned him and his team the prestigious Oman research council's national award for best research.

Deepak Puthal received the Ph.D. degree in computer science from the University of Technology Sydney (UTS), Australia. He is currently a Lecturer at School of Computing, Newcastle University, Newcastle upon Tyne, UK. He has authored in several international conferences and journals, including the ACM and IEEE transactions. His research interests include cyber security, Internet of Things, distributed computing, and edge/fog computing. He is a Program Chair and a TPC member to several IEEE and ACM sponsored conference and symposium. He was a recipient of the 2017 IEEE Distinguished Doctoral Dissertation Award from the IEEE Computer Society and STC on Smart Computing. He served as a Co-Guest Editor of several reputed journals, including Concurrency and Computation: Practice and Experience, Wireless Communications and Mobile Computing, and Information Systems Frontier. He is an Associate Editor of the IEEE Transactions on Bigdata, and IEEE Consumer Electronics Magazine.

Saraju P. Mohanty obtained a Bachelors degree with Honors in Electrical Engineering from the Orissa University of Agriculture and Technology (OUAT), Bhubaneswar, 1995. His Masters degree in Systems Science and Automation is from the the Indian Institute of Science (IISc), Bangalore, in 1999. He obtained a Ph.D. in Computer Science and Engineering (CSE) in 2003, from the University of South Florida (USF), Tampa. He is a Professor at the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by National Science Foundations, Semiconductor Research Corporation, US Air Force, IUSSTF, and Mission Innovation Global Alliance. He has authored 300 research articles, 4 books, and invented 4 US patents. His Google Scholar h-index is 31 and i10-index is 110. He has received 6 best paper awards and has delivered multiple keynote talks at various International Conferences. He received IEEE-CS-TCVLSI Distinguished Leadership Award in 2018 for services to the IEEE, and to the VLSI research community. He was the recipient of 2016 PROSE Award for best Textbook in Physical Sciences & Mathematics category from the Association of American Publishers for his Mixed-Signal System Design book published by McGraw-Hill in 2015. He is the Editor-in- Chief (EiC) of the IEEE Consumer Electronics Magazine. He served as the Chair of Technical Committee on VLSI, IEEE Computer Society during 2014-2018.