Intelligent Automation And Soft Computing, 2019
Copyright © 2019, TSI® Press
Vol.25,no.1,117–119

Guest Editorial:
Advances In Security and Privacy Technologies for Forthcoming Smart Systems, Services, Computing, and Networks

Ilsun You, Chang Choi, Vishal Sharma, Isaac Woungang, and Bharat K. Bhargava

WITH the advancement in the network technology and increase in the number of networked smart devices and distributed information systems, the demand for new emergent services such as smart mobility, smart logistics, and smart homes, is expected to increase. These services aim at facilitating our daily life by supporting mechanisms through automated processing. However, applicability and development of applications on smart services are still in their early days, and many issues require scientific investigation. In particular, the problems of successful implementation of smart services, for which factors like intelligence, mobility, security, and privacy, should be deeply evaluated.

Affected by the potentially great market and future innovations on the application and smart services will increase and deployed rapidly. But this will further raise the requirements of security, privacy, and trust for smart services as well as for the devices supporting such applications.

In this Special Section in AutoSoft journal, different researchers who are working on cognate research issues contributed with their high-quality papers that further advance the understanding of security and privacy technologies for forthcoming smart systems, services, computing, and networks. After rigorous reviews, 9 articles have been accepted in this special issue and we hope that because of wide reachability of this journal, these articles will gain popularity amongst the researchers in the similar domain.

A Critical Infrastructure (CI) can be defined as a combination of essential and irreplaceable services provided to a nation and its people. Halts in the operations of CIs seriously affects many of the important services that citizens, businesses, government agencies, and others rely on to conduct their regular operations. In order to evaluate such an environment, Baig and Zeadally (*Cyber-Security Risk Assessment Framework for Critical Infrastructures*) proposed risk assessment framework focusing on smart grid communications infrastructures. The proposed framework uses the three-step procedure to identify risk and used to quantify and assess existing vulnerabilities in the infrastructure. The framework also evaluates the total risk by including interdependencies between individual components of the CI. This framework is applicable where the details of each level are provided by the stakeholders.

Evaluation of web is another major challenge and identification of anomalies becomes tedious because of the huge size of data being generated in few instances. Guan et al. (*The Design and Implementation of a Multidimensional and Hierarchical Web Anomaly Detection System*) proposed an anomaly detection system, MHWADS, which is designed by considering performance and low latency parameters. The proposed MHWADS obtains the data through each specific domain name and calculates the statistical characteristics and formulates a model. Further, it detects the behavior characteristics of data and finally finds abnormal behavior by using classification algorithms. It uses 2-fold Stacking as the ensemble architecture to gain an effective performance.

Prevention of reverse engineering can help securing the smart applications. It is required that exposure to application root should not be allowed as it may help an attacker gaining access to the entire service network. Lim et al. (*Protecting Android applications with multiple DEX files against Static Reverse Engineering Attacks*) proposed a method to encrypt android application with the multiple DEX files. The encrypted files are stored in the APK files. The proposed method is able to provide protection against static reverse engineering attacks but time overhead is an open issue.

IoT networks operate by enhancing trust amongst its entities. These networks rely on the centralized or distributed nature of the deployed network for preventing any attacks based on the

CONTACT Ilsum You ✉ ilsunu@gmail.com

false reputation. Bordel et al. (*Trust provision in the Internet of Things using transversal blockchain networks*) proposed a theoretical framework for trust in IoT with the help of mathematical formalization. The proposed solution is incorporated into the blockchain networks. The blockchain networks formulate Meta-information and this information is protected by hash functions and divided into chained data blocks for trust provisioning.

With the growth of smart services, the decision making systems become complex and it is required that these decisions should not be influenced by the presence of an unauthorized entity. To resolve such an issue, Shi et al. (*A novel privacy-preserving multi-attribute reverse auction scheme with bidder anonymity using multi-server homomorphic computation*) proposed a privacy-preserving multi-attribute reverse auction scheme. This scheme is based on the Paillier public key cryptosystem with homomorphism. The bidder anonymity is achieved by using oblivious transfer and anonymization techniques. With the reasonable computation cost, the proposed approach is able to determine the privacy-preserving winner with bid privacy.

The usage of GPUs improves the brute force attacks and cryptanalysis on access points of the wireless networks, especially for WiFi networks. It is time-consuming for the cryptanalysis with the huge total combinations of 95^{63}. Chang et al. (*Cracking of WPA & WPA2 Using GPUs and Rule-based Method*) proposed a password cracking scheme based on the rules-based methods. The proposed scheme improves the efficiency of cracking WPA/WPA2 protected access points. Cryptanalysis on these access points is time-consuming. The proposed scheme aims at reducing the time for cracking the password.

Smart services, irrespective of their domain and application area, must be able to provide strong authentication for preventing any misusage. Such a scenario becomes more crucial when biometrics is involved as a part of smart service systems. Choi et al. (*User Authentication System Based on Baseline-corrected ECG for Biometrics*) proposed a User Authentication System which relies on the Baseline-corrected ECG. The proposed system consists of the steps for obtaining ECG lead-I with the developed instrument by removing noise and improve baseline with the primary regression analysis.

Various smart applications depend on visual odometry for processing. Validation of tracking and facilitation of learning are the major requirements of such smart service systems. Lee et al. (*Visual Object Detection and Tracking Using Analytical Learning Approach of Validity Level*) proposed object detection and tracking method to localize and track a visual object in the video stream. The proposed method consists of three methods: object detection, tracking, and learning. The proposed method generates a validity level of object tracking to evaluate whether it moves correctly or not.

Prevention of Denial of Services (DoS) and Distributed DoS (DDoS) is of utmost importance. Any system which is unable to handle the incoming requests is of no use and attacks like DDoS make it extremely difficult for a system to sustain. Chen and Kuo (*Active Detecting DDoS Attack Approach Based on Entropy Measurement for the Next Generation Instant Messaging App on Smartphones*) gave an active detecting approach for DDoS attacks. The proposed approach is based on the entropy measurements. The entropy is emphasized under the active ICMP protocol. The entropy measurement method is used to measure the behavior of the NGIM traffics and numbers of IPv4 and IPv6 addresses.

Finally, we are happy with the technical depth, and reach of this special section, and also hope that it will further advance the understanding in security and privacy technologies for forthcoming smart systems, services, computing, and networks. At last, we want to extend our sincere thanks to all the authors and reviewers for the tremendous efforts, and the Editor-in-Chief and Staff Members for their timely support and guidance.

NOTES ON CONTRIBUTORS

Ilsun You received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, Korea, in 1997 and 2002, respectively. He received the second Ph.D. degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was at the THINmultimedia Inc., Internet Security Co., Ltd. and Hanjo Engineering Co., Ltd. as a research engineer. Now, he is an associate professor at Department of Information Security Engineering, Soonchunhyang University. He has served or is currently serving as a main organizer of international conferences and workshops such as MobiWorld, MIST, SeCIHD, AsiaARES, and so forth. Dr. You is the EiC of Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). He is in the Editorial Board for Information Sciences (INS), Journal of Network and Computer Applications (JNCA), International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Computing and Informatics (CAI), Journal of High Speed Networks (JHSN), Intelligent Automation & Soft Computing (AutoSoft), and Security and Communication Networks (SCN). His main research interests include internet security, authentication, access control, and formal security analysis. He is a Fellow of the IET and a senior member of the IEEE.

Chang Choi received his B.S., M.S. and Ph.D. degrees in Computer Engineering from Chosun University in 2005, 2007, and 2012, respectively. Currently, He is now working as a research professor at the same university. He was awarded the academic awards of graduate school from Chosun University in 2012. Also, he received Korean government scholarship program for graduate students (Ph.D. course) in 2008. Dr. Choi has served or is currently serving on the organizing or program committees of international conferences and workshops such as ACM RACS, EAI BDTA, IE, ACM SAC, IEEE CCNC/SeCHID and so forth. Also, he has served as a guest editor of high-qualified journals such as, Future Generation Computer Systems, Applied Soft Computing, Multimedia Tools and Applications, Journal of Ambient Intelligence and Humanized Computing, Concurrency and Computation: Practice and Experience, Autosoft and so forth. His research interests include Intelligent Information Processing, Semantic Web, Smart IoT System and Intelligent System Security. He is an Associate Editor of IEEE Access and senior member of the IEEE.

Vishal Sharma received the Ph.D. and B.Tech. degrees in computer science and engineering from Thapar University (2016) and Punjab Technical University (2012), respectively. He worked at Thapar University as a Lecturer from Apr'16-Oct'16. From Nov. 2016 to Sept. 2017, he was a joint post-doctoral researcher in MobiSec Lab. at Department of Information Security Engineering, Soonchunhyang University, and Soongsil University, Republic of Korea. Dr. Sharma is now a Research Assistant Professor in the Department of Information Security Engineering, Soonchunhyang University, The Republic of Korea. Dr. Sharma received three best paper awards from IEEE-ICCMIT, Warsaw, Poland in April 2017; from CISC-S'17, South Korea in June 2017; and from IoTaas, Taiwan in September 2017. He is the member of IEEE, a professional member of ACM and past Chair for ACM Student Chapter-Patiala. His areas of research and interests are 5G networks, UAVs, estimation theory, and artificial intelligence.

Isaac Woungang received his Ph.D degree in Mathematics from the University of South, Toulon & Var, France in 1994. From 1999 to 2002, he worked as software engineer at Nortel Networks, Ottawa, Canada. Since 2002, he has been with Ryerson University, Toronto, Canada, where he is now a Professor of Computer Science. His current research interests include radio resource management in next generation wireless networks, BigData, IoT, and Cloud computing. Dr. Woungang has published 8 books and over 90 refereed technical articles in scholarly international journals and proceedings of international conferences. He has served as Associate Editor of the Computers and Electrical Engineering (Elsevier), and the International Journal of Communication Systems (Wiley). He has Guest Edited several Special Issues with various reputed journals such as Computer Communications (Elsevier) and Telecommunication Systems (Springer). Since January 2012, He served as Chair of Computer Chapter, IEEE Toronto Section (2013-2016).

Bharat Bhargava is a professor of computer science at Purdue University. He is conducting research in security and privacy issues in Service Oriented Architecture (SoA) and Cloud Computing. This involves identity management, trust and privacy, secure routing in internet and mobile networks and dealing with malicious hosts, adaptability to attacks, controlled data dissemination, and experimental studies. His recent work involves V2V security and safety, and intelligent autonomous systems and data analytics. Prof. Bhargava has won six best paper awards in addition to the technical achievement award and golden core award from IEEE, and is a fellow of IEEE. He received Outstanding Instructor Awards from the Purdue chapter of the ACM in 1996 and 1998. He has graduated the largest number of PhD students in CS department and is active in supporting/mentoring minority students. He has graduated the largest number of women PhD students and the first African American student PhD in Purdue’s CS department. In 2003, he was inducted in the Purdue's Book of Great Teachers. He is editor-in-chief of four journals and serves on over ten editorial boards of international journals. Professor Bhargava is the founder of the IEEE Symposium on Reliable and Distributed Systems, IEEE conference on Digital Library, and the ACM Conference on Information and Knowledge Management. Bhargava has worked extensively at research laboratories of Air Force and Navy. He has successfully completed several Darpa and Navy STTR and AFRL projects. His recent work on Controlled Data Dissemination in untrusted environments under attacks received the first place in Purdue’s CERIAS security center symposium held in March 2015. This system integrated with secure browser (of MIT W3G.org) for adaptable E2E service configuration and agile defense under various contexts will be demonstrated to clients of NGC Corporation in their Tech-Fest in June, 2015 in McLean, Virginia.