Editorial

Ilsun You*

Department of Information Security Engineering,
Soonchunhyang University,
22 Soonchunhyang-ro, Shinchang-myeon, Asan-si,
Choongchungnam-do 31538, Korea
Email: isyou@sch.ac.kr
*Corresponding author

Jian Weng

College of Information Science and Technology,
Jinan University,
Guangzhou 510632, China
Email: cryptjweng@gmail.com

Zheli Liu

College of Computer and Control Engineering,
Nankai University,
94 Weijin Rd, Nankai Qu 300071,China
Email: liuzheli@nankai.edu.cn

Biographical notes: Ilsun You received his MS and PhD in Computer Science from Dankook University, Seoul, Korea, in 1997 and 2002, respectively. He received his second PhD from Kyushu University, Japan, in 2012. Now, he is an Associate Professor at Department of Information Security Engineering, Soonchunhyang University. 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.

Jian Weng received his MS and BS in Computer Science and Engineering from South China University of Technology, in 2004 and 2000, respectively, and his PhD in Computer Science and Engineering from Shanghai Jiao Tong University, in 2008. From April 2008 to March 2010, he was a Postdoctor in the School of Information Systems, Singapore Management University. He is currently a Professor and Executive Dean with the School of Information Technology, Jinan University. He has published more than 60 papers in cryptography conferences and journals such as Eurocryp, Asiacrypt, PKC, and IEEE TIFS. He served as PC co-chair or PC member for more than ten international conferences.

Zheli Liu received his BSc and MSc in Computer Science from Jilin University, China, in 2002 and 2005, respectively. He received his PhD in Computer Application from Jilin University in 2009. After a Postdoctoral fellowship in Nankai University, he joined the College of Computer and Control Engineering of Nankai University in 2011. Currently, he works at Nankai University as an Associate Professor. His current research interests include applied cryptography and data privacy protection.

Currently, the usage of network and internet services is common and still growing day by day, but at the same time raising various security issues. Networks are under security attacks of various kinds. Extensive attacks can cause a heavy loss in few seconds. Therefore, securing networks is very imperative. Researchers, analysts, designers and developers are taking considerable interest in different aspects of network and internet security (Nazario and Kristoff, 2012; Granjal et al., 2015). Advance security methods and intrusion detection techniques can play a significant role in detecting and preventing security attacks. Reliable security solutions that rely on both in-depth cryptography and secure engineering such as data confidentiality, data integrity, and authentication, non-repudiation, and access control services are required.

In short, providing security in computer communication, network and internet is one of the major challenges of the current age. This special issue is intended to present state-of-the-art research in the area of security for network and the internet. It focuses on advances in cryptography, security engineering and its application issues for network and internet environments. It will also serve as a useful reference for cryptography, security and its applications and will provide readers the most important state-of-the-art technologies in security and dependability of networks.

In this special issue, a total of seven papers were selected after a rigorous review process. These papers addressed the security and privacy issues in network and internet, and proposed efficient solutions for these problems.

The first paper entitled 'ID-based multi-receiver signcryption scheme in the standard model' by Zhimin Yu, Zhengjun Jing, Hua Yang and Chunsheng Gu pointed out that how to ensure secure data transmission and non-repudiation has been a hot issue. In this paper, authors proposed an ID-based multi-receiver signcryption scheme in the standard model based on multilinear maps. In their construction, the number of recipients is unlimited and each receiver decrypts ciphertext using his private key and verifies the identity of the sender. At the same time, the identity-based design has important advantages in that it eliminates the large overhead of having to store and verify a set of verification keys. Based on the hardness assumption of the graded Diffie-Hellman problem, authors proved that the proposed scheme can achieve the message confidentiality under selective multi-ID, chosen message attack and the signcryption is unforgeable under selective ID, chosen message attack.

The next paper entitled 'A smart home foundation scheme based on open source hardware and cloud computing' by Wei Zhou, Jian Xu and Bin Wang proposed a smart home foundation scheme adopting open source hardware devices and cloud computing technology to explore these issues. In this scheme, Arduino Yun-based smart hardware devices can connect to the cloud server through multiply network connectivity. By utilising space brew technology, a bidirectional real time communication can be implemented which provides a solid foundation for real time operations of smart home. The core functions of the scheme are exposed through RESTful web services in software as a service (SaaS) manner and can be called by various clients and other applications. Demonstrative applications show that the proposed smart home foundation scheme provides adequate support for creating smart home applications based on wireless open source hardware devices.

Intrusion detection system (IDS) plays critical role in computer protection systems. Numerous approaches such as machine learning, data mining, and statistical techniques have been examined for IDS task. The third paper entitled 'Performance evaluation of intrusion detection system using classifier ensembles' by Bayu Adhi Tama and Kyung-Hyune Rhee conducted a comparative study of the performance of five renowned ensemble techniques, i.e., bagging, stacking, boosting, rotation forest, and voting, based on three base classifiers, i.e., decision tree (C4.5), convolutional neural network (CNN), and support vector machine (SVM). Based on the experimental results, boosting and stacking perform better than bagging, rotation forest, and voting scheme. In particular, boosting-C4.5 and stacking possess the best performance in terms of performance metrics such as accuracy, precision, recall, and AUC value.

The fourth paper entitled 'Virtual representation of facial avatar through weighted emotional recognition' by Yong-Hwan Lee proposed a novel multiple emotion recognition schemes from facial expressions which is able to understand a combination of different emotions using active appearance model (AAM), k-nearest neighbour (k-NN) and the proposed classification model in mobile environments. To evaluate the performance of the proposed method, authors assessed the ratio of success in real time processing with iPhone camera views. The experimental results show that the proposed method effectively performed well over the recognition of facial emotion, and the obtained result indicates the good performance and enough to applicable to mobile environments.

The fifth paper entitled 'Enhanced security model and efficient construction for direct anonymous attestation' by Xiaohan Yue, Fucai Zhou, Xibo Wang and Rui Li presented the enhanced security model for direct anonymous attestation (DAA), in which more precise security notions demanded from DAA are defined than that in any previous model. Then they proposed a novel approach for constructing an efficient DAA scheme: they designed a secure two-party computation protocol for the join/issue protocol of DAA, and constructed the DAA scheme concretely under the q-SDH assumption, DL assumption and XDH assumption. Based on the enhanced security model, they proved that their DAA scheme meets user-controlled anonymity, user-controlled traceability and non-frame ability in the random oracle model. Finally compared with other existing DAA schemes, they proved that their DAA scheme has better performance.

Distributed denial of service (DDoS) attacks are those which deplete the valuable resource available for the legitimate user, giving them to the malicious user which obviously reduces the business value of any web service provided. This sort of cyber-attacks has to be detected and respective actions have to be taken on them. The challenge is to find the attacking node or network where the attacks are originated, in order to avoid the same in the future or mitigate them. For this, the sixth paper entitled 'A learning-based hybrid framework for detection and defence of DDoS attacks' by T. Subbulakshmi presented an anomaly detection mechanism to generate and detect DDoS attacks using machine learning algorithms and to identify the real IP address of the spoofed attack source using the entropy-based defensive mechanism which is filtered using the IP tables. When the attacks are generated, the entropy values of the various routers are calculated. The network parameters are observed and given as the input to the machine learning algorithms such as back propagation neural network (BPNN), self-organising map (SOM) and enhanced support vector machine (ESVM) to detect the attacks. After the attacks are detected the real source of the attacks and the path in which they are traversed are found out using the entropy values. This helps in filtering the spoofed attack source to defence the attacks from the network. The detection and defence mechanism are found to be effective in identifying the attack source. The detection efficiency is 99% using ESVM. The time required to defend the real attacker IP is less than 2 secs using the entropy-based tracing scheme. The integrated detection and defensive mechanism is found to be better in the field of DDoS attack detection and defence.

Finally, the seventh paper entitled 'Categorisation of web pages for protection against inappropriate content in the internet' by Igor Kotenko, Andrey Chechulin and Dmitry Komashinsky outlined a framework for automated categorisation of web pages to protect against inappropriate content. The paper contains the framework overview, analysis of state-of-the-art, description of the developed prototype and its evaluation based on series of experiments. Several sources are used for the categorisation, namely text, html tags and URL addresses. During the categorisation, this data and other information are analysed using machine learning and data mining methods. Finally, the evaluation of the categorisation quality is performed. The categorisation system developed as a result of this work are planned to be partially implemented in F-secure corporation in mass production systems performing analysis of web content.

We hope that the seven papers presented in this special issue will make a significant contribution to academic researchers, industry professionals, students, and all the interested readers of this subject, working to extend their knowledge in the areas of security and dependability of networks and internet.

Finally, we would also like to express our sincere appreciation and thanks to all the authors for their valuable contributions. Our special thanks go to the editorial board for this special issue, Jiann-Liang Chen and Sherali Zeadally, Editors-in-Chief of the *International Journal of Internet Protocol Technology*, for this kind invitation to organise this issue and the great support provided by them throughout the entire publication processes.

References

Granjal, J., Monteiro, E. and Silva, J.S. (2015) 'Security for the internet of things: a survey of existing protocols and open research issues', *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 3, pp.1294–1312.

Nazario, J. and Kristoff, J. (2012) 'Internet infrastructure security', *IEEE Security & Privacy*, Vol. 10, No. 4, pp.24–25.