Guest Editorial: Emerging Security Technologies and Applications*

Fang-Yie Leu
Computer Science Department
Tunghai University, Taichung, Taiwan
leufy@thu.edu.tw

Due to the quick increase in number of mobile, ubiquitous, cloud, network and communication applications and studies, many computer and communication systems, wired or wireless, have been released to service their customers (human users or other systems). However, hackers everywhere around the world may attack these systems for some reasons, e.g., stealing one company's business secrets for another one, penetrating a system to show the achievement of their professional skills, preventing a system from providing its regular/normal services just for fun, etc. To safely guard a system from being attacked or intruded, we need security mechanisms to protect our systems and the information delivered between/among the systems. That is why information security has been an important issue in recent computer and communication research. It is also why this special issue is created. This special issue collects a series of papers that discuss different aspects of emerging security technologies and applications. The focus of the selected articles mainly on technical approaches to prevent a system from being attacked, and on techniques for encrypting messages/information delivered between two communication entities.

The first article [1], "Efficient and Low-Cost RFID Authentication Schemes" by Atsuko Miyaji, Mohammad Shahriar Rahman and Masakazu Soshi, presents two mutual RFID authentication protocols aiming to improve YA-TRAP* by preventing the system being considered from a timing attack, and by providing RFID with a RFID reader authentication. The two protocols also achieve other security properties like forward security, resistance against cloning, replay, and tracking attacks. Moreover, the computation and communication costs are kept as low as possible for the tags. In fact, it is important to keep the communication cost as low as possible when many tags are authenticated in batch-mode. By introducing an aggregate function for the reader-to-server communication, the communication cost is reduced.

The second article [2], "Enhancing SVO Logic for Mobile IPv6 Security Protocols" by Ilsun You, Yoshiaki Hori and Kouichi Sakura, studies the formal analysis on the security protocols for MIPv6, particularly focusing on modal logic. Especially, the authors extend the SVO logic, which is one of the most mature and successful modal logic techniques, to precisely analyze MIPv6 security protocols. The proposed logic is applied to analyze the four security protocols, including CAM, ERO, KKP, and YHSP, to show its effectiveness in precisely reasoning about their security.

The next article [3], "A Lightweight Security Framework for Wireless Sensor Networks" by Tanveer A. Zia and Albert Y. Zomaya, proposes a computationally lightweight security framework to provide WSNs with a comprehensive security solution against the known attacks. The framework consists of four interacting components: a secure triple-key scheme, secure routing algorithms, a secure localization technique and a malicious node detection mechanism, each of which can achieve a certain level of security. The framework takes into consideration the communication and computation limitations of sensor networks. Generally, there is always a tradeoff between security and performance. The authors claim that the experimental results prove that the framework can achieve a high degree of security with negligible overheads.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 2, number: 3, pp. 1-3

*This special issue is financially supported by Database and Network Security lab. at Tunghai University, Taiwan (directed by Prof. Fang-Yie Leu, http://dblab.csie.thu.edu.tw).

In [4], “A Proxy E-Raffle Protocol based on Proxy Signatures” by Nasrollah Pakniat and Ziba Eslami, the authors propose an efficient proxy raffle scheme which overcomes the weakness existing in the approach introduced by Chang and Cheng based on the concept of proxy signatures and symmetric cryptography, and conclude that the proposed scheme achieves all other security requirements mentioned in the literature, and outperforms the Chang-Cheng’s one in terms of communication load and computational complexity.

The next article [5], “Mobile Banking Payment System” by Fuw-Yi Yang, Zhen-Wei Liu and Su-Hui Chiu, presents a new payment system, called the mobile banking payment system, with which customers do not require to purchase e-money of a fixed value in advance. The amount of the payment of a transaction is deducted directly from the customer’s bank account, thus eliminating the inconvenience of fixed value currency, and reducing online computing requirements. Through the application of trapdoor hash functions to streamline computational processes, the system can be used with mobile devices.

The last one [6], “Constructing a Secure Point-to-Point Wireless Environment by Integrating Diffie-Hellman PKDS, RSA and Stream Ciphering for Users Known to Each Other” by Yi-Li Huang and Fang-Yie Leu, proposed an authentication approach, called the secure point-to-point encryption method (SePem for short), which integrates RSA, Diffie-Hellman PKDS and a stream cipher technique to provide users with a highly secure point-to-point wireless network without requiring a CA. The authors claim that according to their security analysis, the SePem can efficiently and securely protect a wireless environment, and the simulation results show that the performance of this method can meet users’ communication needs.

Although the articles selected in this special issue address several important aspects of emerging security technologies and applications, many security areas and topics need to be intensively enhanced and developed, like how to effectively prevent, rather than detect, DoS and DDoS attacks, how to trace back to the real attacking nodes once a stepping stone is used, how to detect and avoid an insider attack, etc. I hope these threatens can be solved one by one in the near future. At last, I would like to extend my special thanks to Dr. Ilsun You who is the Editor-in-Chief of *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. Without his invitation and help, this special issue cannot be published on time.

Fang-Yie Leu
Guest Editor
September, 2011

References

[1] A. Miyaji, M. S. Rahman, and M. Soshi, “Efficient and low-cost RFID authentication schemes,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 3, pp. 4–25, September 2011.

[2] I. You, Y. Hori, and K. Sakura, “Enhancing SVO logic for Mobile IPv6 security protocols,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 3, pp. 26–52, September 2011.

[3] T. A. Zia and A. Y. Zomaya, “A lightweight security framework for wireless sensor networks,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 3, pp. 53–73, September 2011.

[4] N. Pakniat and Z. Eslami, “A proxy e-raffle protocol based on proxy signatures,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 3, pp. 74–84, September 2011.

[5] F.-Y. Yang, Z.-W. Liu, and S.-H. Chiu, “Mobile banking payment system,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 3, pp. 85–95, September 2011.

[6] Y.-L. Huang and F.-Y. Leu, “Constructing a secure point-to-point wireless environment by integrating Diffie-Hellman PKDS, RSA and stream ciphering for users known to each other,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 3, pp. 96–107, September 2011.

Fang-Yie Leu received his BS, master and Ph.D. degrees all from National Taiwan University of Science and Technology, Taiwan, in 1983, 1986 and 1991, respectively, and another master degree from Knowledge System Institute, USA, in 1990. His research interests include wireless communication, network security, Grid applications and Chinese natural language processing. He is currently a professor of TungHai University, Taiwan, and director of database and network security laboratory of the University. He is also a member of IEEE Computer Society. insider threats in organisations.