J Ambient Intell Human Comput (2013) 4:207–208
DOI 10.1007/s12652-011-0101-z

EDITORIAL

Special issue on cloud, wireless and e-commerce security

Fang-Yie Leu · Chu-Hsing Lin · Aniello Castiglione

Published online: 31 December 2011

In recent years, the increase in number of cloud computing, wireless network and e-commerce applications has triggered many security studies and also faced many pivotal challenges including integrity verification, authentication, access control, attack prevention, etc., which are basically current emerging issues needed to be effectively solved to make modern computer/network environments more secure than before. However, the nature and scope of the security fields have quickly evolved. Hackers surround us anytime and anywhere. Even though many related technologies have been developed and a huge number of security problems have been solved, security challenges still exist nowadays, consequently threatening modern cyber-systems both in academia and industry. In other words, efforts are still required in security studies. To achieve the whole security target for cloud computing, wireless network and e-commerce, it requires much more than the mere applications of current core technologies and theories. The aim of this special issue is to address different aspects of cloud, wireless and e-commerce security technologies and applications. The focuses of the papers selected from the international workshop of Cloud, Wireless and e-Commerce 2011 (CWECS 2011) are mainly on technical approaches to prevent a system from being attacked, and on techniques for encrypting messages/information delivered between two communication entities. In the first paper by Lin et al., the authors introduced a novel protocol named Fast Iterative Localized Re-authentication (FIL Re-authentication) to replace the fast re-authentication in EAP-AKA protocol. FIL Re-authentication makes use of iterative process and localized re-authentication process for speeding up re-authentication times and reducing Intra-domain handover authentication delays in 3G/UMTS-WLAN interworking networks. The performance evaluation shows that proposed protocol surpasses standard EAP-AKA protocol in terms of authentication session time, authentication delay and handover authentication delay. The second paper by De Santis et al. presents a new active and scalable firewalling architecture based on dynamic and adaptive policy management facilities to enable the automatic generation of new rules and policies so as to ensure a timely response in detecting unusual traffic activity as well as identify unknown potential attacks (zero-day). The proposed scheme, with a multi-stage modular structure, can be easily applied to a distributed security environment and does not depend on any specific security solutions or hardware/software packages. The third one by Camastra et al. investigates the trends of the Machine Learning (ML) and Soft Computing (SC) methodologies for Information and Communication Technology (ICT) security. In particular, this paper overviews ML and SC applications for three hot topics in ICT security, including password-based schemes for access control, intrusion detection and spam filtering. It has been shown that ML and SC have been widely applied in ICT security, due to the fact that they allow a system to reply to changeable real-world inputs and learn to identify undesirable behaviors. In this way, the authors show that ML and SC are becoming more and more a very important tool for Computer Security. Unlike other

F.-Y. Leu (✉) · C.-H. Lin (✉)
Department of Computer Science, Tunghai University,
No. 181, Section 3, Taichung Port Road, Taichung, Taiwan
e-mail: leufy@thu.edu.tw

C.-H. Lin
e-mail: chlin@thu.edu.tw

A. Castiglione (✉)
Dipartimento di Informatica, Università degli Studi di Salerno,
Via Ponte don Melillo, 84084 Fisciano, SA, Italy
e-mail: castiglione@ieee.org; castiglione@acm.org

ML and SC applications, the ones in the Computer Security have to work under adversarial conditions. Adversarial conditions mean, for instance, that an attacker can attempt to use the adaptive aspect of ML and SC systems to cause them to fail. The authors conclusions are that developing secure learning algorithms, i.e., algorithms that can work under more disparate adversarial conditions, is a big challenge for ML and SC researchers in the next future.

In the fourth paper, Yang et al. proposed an effective RSA multi-signature scheme based on Shamir's identity-based signature (IBS) scheme, where its signature length is comparable with that of Shamir's IBS scheme. Also, only one/two extra increments of $l - 1$ modular multiplications are added to the verification/signature time, whereby l represents the number of signers. This greatly reduced the computational load and communication costs compared to the previously proposed multi-signature schemes. This research analyzing the origins of loopholes, enhances the original schemes by preserving the advantages of the scheme and obtain an enhanced overall security. The proposed protocol, resultant from the improvements added by the authors, is thus well qualified for wireless networking due to it not only having strong security but also because it saves computational resources and communication bandwidth.

In the fifth paper, Yang and Liang reviewed Liu et al.'s scheme and its security loopholes, and then proposes a proxy partially blind signature scheme. In fact, while the Liu et al.'s scheme can revoke the proxy privileges and authentication of previous blind signatures, it lacks the untraceability and unforgeability characteristics required for a good blind signature scheme. The proposed scheme not only retains the revocation functions proposed in Liu et al.'s approach, but also meets the security requirements of proxy blind signatures such as untraceability, unforgeability. The sixth paper by Castiglione et al. presented an extended experimental evaluation on one of the most effective source camera identification techniques proposed by Lukáš et al. This evaluation uses the characteristic noise left by the sensor on a digital picture as a fingerprint to identify the source camera taking the picture, aiming to assess the effectiveness of this technique when used with pictures that were previously modified using several common image-processing functions coming with photo-editing tools. The technique was also applied to photos passed through Online Social Networks or Online Photo Sharing websites, without any "human" explicit modification, but only elaborated by such Web 2.0 tools. The last paper by Lin et al. focuses on the defense mechanism for distributed denial of service (DDoS) attacks. DDoS attacks use a lot of request packets or garbage packets to occupy network bandwidth and lower performance of the target host. If the target host is a commercial website, DDoS attacks will lengthen the transmission delays, and more seriously they will deny web services. From the experimental results, the Double Check Priority Queue (DCPQ) scheme is found to be very effective against DDoS attacks. Its performance is proven to be better than the Priority Queue (PQ) and DropTail schemes. Since it is not possible to completely prevent networks from attacks, the authors only propose to minimize damage caused by DDoS attacks. For that, they use a Double Check Priority Queue (DCPQ) scheme to efficiently alleviate effect of various numbers of DDoS attacks with different packet rates and which maintain a reasonable quality of service for normal users.

Although the papers selected in this special issue address several important aspects of cloud, wireless and e-commerce Security technologies and applications, many security domains and topics need to be intensively enhanced and developed, like how to effectively perform wireless handover authentication, how to effectively prevent DoS and DDoS attacks, how to detect and avoid insider attacks, etc. We wish these threatens can be solved in the near future. Moreover, the Guest co-Editors would like to thank all the authors of this special issue for the efforts they put in the preparation of their manuscripts and for their valuable contributions. We also wish to express our deepest gratitude to the referees for their thorough detailed reviews.

At last, our sincere thanks go to the Editor-in-Chief, Professor Vincenzo Loia, of the Journal of Ambient Intelligence and Humanized Computing for his exceptional support and assistance provided throughout the entire process that led to the publication of this special issue.