Message from the Guest Editors

Jianying Zhou · Xuejia Lai · Hui Li

Published online: 2 August 2012
© Springer-Verlag 2012

In this special issue of International Journal of Information Security, you will find three papers selected from 25 papers accepted by the 14th Information Security Conference (ISC 2011), which was held on October 26–29, 2011, in Xi'an, China. The conference was sponsored by China Computer Federation (CCF) and co-organized by Xidian University and Shanghai Jiao Tong University.

In response to the call for papers, 95 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty, technical quality, and practical impact. Each paper was reviewed by at least three members of the program committee, and the reviewing process was “double-blind.” Finally, 25 papers were selected for presentation at the conference.

Three papers included in this special issue are distinct from the conference version in that they include substantial additional content. Moreover, they had to undergo another round of review to ensure the journal quality. We would like to thank all people contributed in evaluating and elaborating these three journal articles, Xiaofeng Chen, Masahiro Mambo, Chris Mitchell, Peng Ning, Haining Wang, and Yanjiang Yang.

J. Zhou (✉)
Institute for Infocomm Research, 1 FusionopolisWay,
#21-01 Connexis, South Tower, Singapore 138632, Singapore
e-mail: jyzhou@i2r.a-star.edu.sg

X. Lai
Department of Computer Science and Engineering,
Shanghai Jiao Tong University, 800 Dongchuan Road,
Min Hang, 200240 Shanghai, China
e-mail: lai-xj@cs.sjtu.edu.cn

H. Li
Key Laboratory of Computer Networks and Information Security,
Xidian University, 2 South Taibai Road, Xi'an, 710071 Shaanxi, China
e-mail: lihui@mail.xidian.edu.cn

In the paper *Replacement Attacks: Automatically Evading Behavior Based Software Birthmark*, which received the best paper award in ISC 2011, Xin et al. analyzed the weaknesses in the state-of-the-art technology on software birthmark that adopts dynamic system call dependence graphs as the unique signature of a program and constructed replacement attacks with the help of semantics equivalent system calls to unlock the high frequency dependencies between the system calls in the victim's original system call dependence graph. Their results show that the proposed replacement attacks can destroy the original birthmark successfully.

In the paper *Minimizing Information Disclosure to Third Parties in Social Login Platforms*, which received the best student paper award in ISC 2011, Kontaxis et al. designed and developed a framework for minimum information disclosure in social login interactions with third-party sites. Their example case is Facebook, which combines a very popular single sign-on platform with information-rich social networking profiles. Whenever users want to browse to a website that requires authentication or social interaction using a Facebook identity, their system employs, by default, a Facebook session that reveals the minimum amount of information necessary. Users have the option to explicitly elevate that Facebook session in a manner that reveals more or all of the information tied to their social identity. This enables users to disclose the minimum possible amount of personal information during their browsing experience on third-party websites.

In the paper *The n -Diffie-Hellman Problem and Multiple-Key Encryption*, Chen et al. extended the twin Diffie-Hellman (twin DH) problem proposed by Cash, Kiltz, and Shoup to the n -Diffie-Hellman (n -DH) problem for an arbitrary integer n and proved that this new problem is at least as hard as the ordinary DH problem. They also observed that the

double-size key in the Cash et al. twin DH-based encryption scheme can be replaced by two separated keys each for one entity, resulting in a 2-party encryption scheme that holds the same security feature as the original scheme but removes the key redundancy. They further extended this idea to an

n -party case, which is also known as n -out-of- n encryption and presented a variant of ElGamal encryption and a variant of Boneh-Franklin IBE, both of which are efficient as the size of their ciphertext is independent to the value n .