Int. J. Inf. Secur. (2011) 10:267–268
DOI 10.1007/s10207-011-0131-8

EDITORIAL

Message from the Guest Editors

Sushil Jajodia · Jianying Zhou

Published online: 25 May 2011

This special issue of the International Journal of Information Security is devoted to the best papers of the 6th International Conference on Security and Privacy in Communication Networks (SecureComm 2010), held on September 7–9, 2010, in Singapore.

In response to the call for papers, 112 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by at least three members of the program committee. Finally, 28 papers were selected for presentation at the conference, giving an acceptance rate of 25%.

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 by at least two leading security experts to ensure the journal quality.

In the paper "SAS: Semantics Aware Signature Generation for Polymorphic Worm Detection," Kong et al. propose a novel semantics aware statistical algorithm for automatic signature generation. When SAS processes packets in a suspicious flow pool, it uses data flow analysis techniques to remove non-critical bytes and then applies a hidden Markov model (HMM) to the refined data to generate state-transition-graph-based signatures. Their experiments show that the proposed technique can accurately detect worms with concise signatures and that SAS is more robust to the byte distribution changes and noise injection attacks compared to Polygraph and Hamsa.

In the paper "Enhancing Host Security using External Environment Sensors," Chang et al. propose a framework that uses (external) environment information to enhance computer security. The benefit of this framework is that the environment information is collected by sensors that are outside the control of a host and communicate to an external monitor via an out-of-band channel; thus, it cannot be compromised by malware on a host system. The information gathered still remains intact even if malware uses rootkit techniques to hide its activities. This framework can be applied for a number of security applications like intrusion detection, rate monitoring/control of external resources, and access control. They show that that the framework is useful even with coarse-grained and simple information. They also describe some experimental prototypes that employ the framework to detect/control email spam, detect/control DDoS zombie attacks, and detect misuse of compute resources.

In the paper "CASSANDRA: A Probabilistic, Efficient, and Privacy Preserving Solution to Compute Set Intersection," Marconi et al. propose a toolbox composed of three probabilistic protocols that allow two parties, each one having a subset of elements drawn by a pre-determined set, to compute information about the intersection of such two sets. Other than in functionality, these protocols also differ in the degree of assurance they provide and in the degree of interactions required by the two parties. The communication cost also differs, but below the cost of competing solution representing the state of the art. These protocols also share some common features: They are completely tunable and specifically suited for devices having constraints on energy, communication, storage, and bandwidth.

S. Jajodia
George Mason University, Fairfax, USA
e-mail: jajodia@gmu.edu

J. Zhou (✉)
Institute for Infocomm Research, Singapore, Singapore
e-mail: jyzhou@i2r.a-star.edu.sg

We are grateful to the authors who agreed to revise their papers and external reviewers for their hard work during the review process. Eiji Okamoto, Dieter Gollmann, and Javier Lopez, editors-in-chief of this journal, deserve our special thanks for their support.