Journal of Computer Security 15 (2007) 1–2
IOS Press

Message from the Guest Editors

Ad-hoc and sensor networks are expected to become an integral part of the future computing landscape. However, these networks introduce new security challenges due to their dynamic topology, severe resource constraints, and absence of a trusted infrastructure. This Journal of Computer Security (JCS) special issue is intended for academia and industry researchers to share their recent research on security for ad-hoc and sensor networks.

We received quite a few submissions to this special issue. We would like to thank all the authors for sending their outstanding work to this special issue. However, due to the space constraints, we were only able to accept a small fraction of these excellent papers.

This special issue includes six excellent papers that cover a variety of topics, including trust establishment in Mobile Ad-Hoc Networks (MANETs), security of vehicular ad-hoc networks, secure aggregation in sensor networks, detecting misbehaviors in ad-hoc networks, secure group communication, and distributed signature protocols for ad-hoc networks.

Zouridaki, Mark, Hejmo, and Thomas propose a trust establishment scheme for MANETs which aims to improve the reliability of packet forwarding over multi-hop routes in the presence of potentially malicious nodes. The proposed scheme uses a Bayesian framework; each node forms an "opinion" about each of the other nodes in the network, based on the set of trustworthiness values computed in the network.

The paper by Raya and Hubaux addresses the security of vehicular networks. It provides a detailed threat analysis in vehicular networks; it devises an appropriate security architecture, and identifies some major design decisions still to be made. The paper also provides a set of security protocols to protect vehicular networks.

Chan, Perrig, Przydatek, and Song propose a novel framework for secure information aggregation in large sensor networks. By constructing efficient random sampling mechanisms and interactive proofs, the framework enables the querier to verify that the answer given by the aggregator is a good approximation of the true value, even when the aggregator and a fraction of the sensor nodes are corrupted.

Radosavac, Cárdenas, Baras, and Moustakides consider the problem of detection and prevention of node misbehavior at IEEE 802.11 MAC layer in ad-hoc networks. The paper focuses on the back-off manipulation by selfish nodes. It proposes an algorithm that ensures honest behavior of non-colluding participants; it also analyzes the problem of colluding selfish nodes, casting the problem within a minimax robust detection framework and providing an optimal detection rule for the worst-cast attack scenarios. The paper indicates that the approach is general and can be used with any probabilistic distributed MAC protocol.

The paper by Xu demonstrates that several group communication schemes used by both wired networks and MANETs are vulnerable to an attack that allows an outside

adversary who has compromised a certain legitimate group member to obtain all past and present group keys. This is in sharp contrast to the widely-accepted belief that such an adversary can only obtain the present group key. The paper also shows that some practical methods can make a subclass of existing group communication schemes immune to the attack.

Finally, the paper by Zanin, Di Pietro, and Mancini proposes a distributed RSA signature protocol for large-scale, long-lived ad-hoc networks. The scheme guarantees that an adversary can neither forge a signature nor disrupt the computation, unless it has compromised at least t nodes of different classes. Moreover, an attempt to disrupt the distributed service, by providing fake information, would reveal the cheating node.

Putting together this special issue was a team effort. We would like to express our gratitude to the external reviewers, who worked very hard in reviewing the papers and providing suggestions for their improvements. We would also like to thank the JCS Editors-in-Chief, Professor Sushil Jajodia and Dr. Jonathan Millen. This special issue would not be possible without their support. We are grateful to Kim Willems, Dovile Skiriute, Tomas Martisius, and possibly others at IOS Press who helped us put this special issue together.

We hope that you will find this special issue interesting and thought-provoking.

Peng Ning and Wenliang Du
Guest Editors, Special Issue on
Security of Ad-hoc and Sensor Networks