Preface

Feng Bao*

Institute for Infocomm Research, Singapore
E-mail: baofeng@i2r.a-star.edu.sg
*Corresponding author

Colin Boyd

Queensland University of Technology, Australia
E-mail: boyd@isrc.qut.edu.au

Dieter Gollmann

Technische Universität Hamburg-Harburg, Germany
E-mail: diego@tu-harburg.de

Kwangjo Kim

Information and Communications University, Korea
E-mail: kkj@icu.ac.kr

Kaoru Kurosawa

Ibaraki University, Japan
E-mail: kurosawa@cis.ibaraki.ac.jp

Masahiro Mambo

Tsukuba University, Japan
E-mail: mambo@cs.tsukuba.ac.jp

Chris Mitchell

Royal Holloway, University of London, UK
E-mail: c.mitchell@rhul.ac.uk

Yi Mu

University of Wollongong, Australia
E-mail: ymu@uow.edu.au

Phillip Rogaway

University of California, Davis, USA
E-mail: rogaway@cs.ucdavis.edu

Willy Susilo

University of Wollongong, Australia
E-mail: wsusilo@uow.edu.au

Vijay Varadharajan

Macquarie University, Australia
E-mail: vijay@ics.mq.edu.au

Moti Yung

Columbia University, USA
E-mail: moti@cs.columbia.edu

Fangguo Zhang

Sun Yat-Sen University, China
E-mail: isdzhfg@zsu.edu.cn

Computer networks play an important role on connecting resources and people. Advances of computer technology have been pushing forward computer networks for high speed and broad bandwidth. Security must be enforced to suit the emerging technologies. With the emergence of wireless technologies, such as IEEE 802.11 and Bluetooth, mobile users are enabled to connect to each other wirelessly. It can be realised with or without any networking infrastructure (ad hoc mode). Wireless access networks are rapidly becoming a part of our everyday life. However, the security concerns remain a serious impediment to widespread adoption. The underlying radio communication medium for wireless network provides serious exposure to attacks against wireless networks. Research on security in computer networks and mobile systems covers many issues. There are many open issues to be solved. Areas of interest for this special journal issue mainly include the following topics: ad hoc network security, authentication in network and wireless systems, cryptographic algorithms and applications, denial of service, distributed system security, encryption in network and wireless systems, fast cryptographic algorithms and their applications, firewall and distributed access control, identity-based cryptography in network and mobile applications, intrusion detection and response, key management, multicast security, mobile communications security, privacy protection, wireless security and algorithms, secure routing protocols and security in peer-to-peer networks.

We received 70 manuscripts. Eight manuscripts were selected for this Special Issue. The reviewing process took eight weeks. Each manuscript was reviewed by normally three (some of them two or four) reviewers consisting of guest editors and external reviewers.

The first paper in this Special Issue: A security solution for IEEE 802.11's ad hoc mode: password-authentication and group-Diffie–Hellman key exchange, is by E. Bresson, O. Chevassut and D. Pointcheval. This work addresses authentication issues in IEEE 802. It leverages the latest developments in the area of password-based authentication and (group) Diffie–Hellman key exchange to develop a provably-secure key-exchange protocol for IEEE 802.11's ad hoc mode. The protocol allows users to securely join and leave the wireless group at time, accommodates either a single-shared password or pairwise-shared passwords among the group members or at least with a central server; achieves security against dictionary attacks in the ideal-hash model (i.e. random-oracles). The first such protocol to appear in the cryptographic literature.

The second paper in this Special Issue: Security mechanisms and vulnerabilities in the IEEE 802.15.3 wireless personal area networks, is by W. Stewart, Y. Xiao, B. Sun and H-H. Chen. This work gives a survey on various security aspects and mechanisms in the IEEE 802.15.3 WPANs. It provides security analysis, points out some errors and security vulnerabilities of these networks and provides some corrections.

The third paper in this Special Issue: The performance of a watchdog protocol for wireless network security, is by J.W. Lee, Y-H. Lee and V.R. Syrotiuk. This work proposes two protocols to address the ambiguous collision limitation of watchdogs. The Watchdog Alert and Watchdog Confirmation protocols are variants of the carrier sense multiple access with collision avoidance protocol (CSMA/CA). It analyses the trade-offs between throughput and watch-dog success probability of each protocol, comparing it to CSMA/CA.

The fourth paper in this Special Issue: A hybrid data mining anomaly detection technique in ad hoc networks, is by Y. Liu, Y. Li, H. Man and W. Jiang. This work proposes a hybrid data mining anomaly detection technique for node-based IDS. Specially, it incorporates two data mining techniques, that is, association-rule mining and cross-feature mining, to characterise normal behaviours of mobile nodes and detect anomalies by finding deviance from the norm. It investigates the feature of interest from both medium access (MAC) layer and network layer. To preserve the precious energy of mobile nodes, it proposes two compact feature sets, that is, direct feature set and statistical feature set, that target on short-term and long-term profiling of normal node behaviours, respectively.

The fifth paper in this Special Issue: Automated detection and containment of worms and viruses into heterogeneous networks: a simple network immune system, is by F. Palmieri and U. Fiore. This work presents a cooperative immunisation system inspired in principles and structure by the natural immune system. The proposed system automatically detects pathologic traffic conditions due to an infection and informs, according to a cooperative communication principle, all the reachable networked nodes about the ongoing attack, triggering the actions required to their defence. To evaluate the proposal, the authors formulated a simple worm propagation and containment model, based on the above principles and

evaluated their system using numerical solution and sensitivity analysis. Their measurements show that the reaction strategy is sufficiently robust against viruses, worms and malicious participants in the network immunisation system. Their solution will be an effective and challenging line of defence against next-generation more aggressive worms.

The sixth paper in this Special Issue: Denial of service resistance in key establishment, is by J. Smith, S. Tritilanunt, C. Boyd, J.M. Gonzalez Nieto and E. Foo. This work reviews the strategies and techniques used to improve resistance to denial of service attacks. Three key establishment protocols implementing denial of service resistance techniques are critically reviewed and the impact of misapplication of the techniques on denial of service resistance is discussed. Recommendations on effectively applying resistance techniques to key establishment protocols are made.

The seventh paper in this Special Issue: DDoS: Design, implementation and analysis of automated model, is by U.K. Tupakula, V. Varadharajan, A.K. Gajam, S.K. Vuppala and P.N.S. Rao. The focus of this work is twofold: firstly, to present a detailed description of the design and implementation of the proposed model and secondly to discuss and analyse the extensive set of results obtained from the implementation and simulations. The authors describe the prototype implementation of our automated model using NetProwler Network Intrusion Detection System (NIDS) and HP OpenView Network Node Manager (NNM). They also discuss the performance analysis of our model on a large scale using NS2 tool. Their system offers several unique advantages over existing schemes.

The eighth paper in this Special Issue: Grain: a stream cipher for constrained environments, is by M. Hell, T. Johansson, W. Meier and F.H. Aargau. They proposed a new stream cipher, Grain. The design targets hardware environments where gate count, power consumption and memory is very limited. It is based on two shift registers and a non-linear output function. The cipher has the additional feature that the speed can be increased at the expense of extra hardware. The key size is 80 bits and no attack faster than exhaustive key search has been identified. The hardware complexity and throughput compares favourably to other hardware oriented stream ciphers like E0 and A5/1.

Finally, we would like to thank the following external reviewers for their invaluable contributions to the reviewing process: Venkat Balakrishnan, Andrew Clark, Ernest Foo, Yi Gao, Xinyi Huang, Miyuki Imada, Atsuo Inomata, Kouichi Itoh, Tetsu Iwata, Shigetomo Kimura, Hui Li, Tieyan Li, Ching Lin, Miao Ma, Masashi Mitomo, Toshio Miyachi, Yuko Murayama, Koji Nakao, Mirang Park, Yasuhiro Ohtaki, Jason Reid, Chun Ruan, Ryoichi Sasaki, Yoshimitsu Shimojo, Makoto Sugita, Uday Tupakula, Ryuya Uda, Zhiguo Wan, Changji Wang, Jian Weng, Dai Watanabe, Baodian Wei, Jian Weng and Shidi Xu. We would like to thank the Editor-in-Chief, Professor Laurence T. Yang for giving us this great opportunity of organising this Special Issue.