Journal of Computer Security 14 (2006) 389–390
IOS Press

Preface

This special issue of JCS is dedicated to the *4th International Workshop for Applied PKI (IWAP'05)* that took place in Singapore, from 21st to 23rd September 2005, in conjunction with the *8th Information Security Conference (ISC'05)*. It contains four papers, of which three were selected from the proceedings of *IWAP'05* and one is based on the keynote speech at *IWAP'05*. The workshop papers were further reviewed and revised for this issue.

Over the past years, *Public Key Infrastructure (PKI)* technology has evolved and moved from the research laboratories to the mainstream, where many organizations are now leveraging it as part of their core infrastructure for providing and building security in their businesses. Understanding the challenges and requirements of *PKI*-related operations through the sharing of case studies is critical to support the continued research and development of *PKI* technologies and related systems and applications, and to enhance future development and evolution of *PKI* in enterprises.

The International Workshop for Applied PKI (IWAP) is an annual workshop that was initiated in 2001 with the objective of focusing on research and application of Public Key Infrastructure. *IWAP'05* provided a good platform for individuals from academia and industry working with PKI to foster exchange of ideas. The proceedings of *IWAP'05* were published by IOS Press, and 18 papers from 11 countries are included. The workshop had one keynote speech and six technical sessions, covering the topics of PKI Operation & Case Study, Non-repudiation, Authorization & Access Control, Authentication & Time-Stamping, Certificate Validation & Revocation, and Cryptographic Applications.

As program chairs, we are indebted to our program committee members and the external reviewers for their valuable contribution to the workshop and this publication. We would like to thank general chairs Feng Bao and Hwee-Hwa Pang for their support and encouragement, and the local organizing team for their dedication and hard work for making the workshop and this publication possible. We would also like to extend our appreciations to all the authors who shared valuable insights and outcome of their researches through their papers and presentations, and last but not least, the participants from all over the world for their attendance. We are also grateful to the Institute for Infocomm Research and Microsoft Asia Pacific for sponsoring the workshop.

The four papers included in this special issue are extended versions of the workshop papers. The first paper is "*Public Key Infrastructures: A Research Agenda*" by Geraint Price. It categorizes some of the challenges facing those building, deploying and using Public Key Infrastructures. Its work is based on a series of in-depth interviews and analysis. The aim of the work in this paper is twofold: to present the conclusions drawn from years of practical experience of those in the field; and to

analyze those conclusions in order to highlight research avenues that will answer the challenges raised by those in industry.

The second paper is "*Life-Cycle Management of X.509 Certificates Based on LDAP Directories*" by M. Lippert, V. Karatsiolis, A. Wiesmaier and J. Buchmann. It highlights the fact that synchronization of the certificates' life-cycles with the management of the *PKI* users is a common problem, and proposes a mechanism to achieve this synchronization based on directory services. This enables transparent updates to the information provided by the *PKI* and offers a high potential for automation. The mechanism spares personnel and is less error-prone, since it relies on processes and data that are already established. It reduces the costs to bootstrap and operate the infrastructure. The paper also shows a case study on the proposed mechanism that was conducted at the Technische Universität Darmstadt in Germany in order to supply 20,000 students with certificates and keys.

The third paper is "*Generic Non-Repudiation Protocols Supporting Transparent Off-line TTP*" by Guilin Wang. A non-repudiation protocol enables the fair exchange of an electronic message and an irrefutable digital receipt between two mistrusting parties over the Internet. This paper argues the importance of generic fair non-repudiation protocols with a transparent off-line trusted third party (TTP), in which each involved party could use any secure digital signature algorithm to produce non-repudiation evidence, and the issued evidence is the same regardless of whether the TTP is involved or not. Then, it presents one such fair non-repudiation protocol to overcome some limitations and shortcomings in previous schemes. Some potential extensions are also pointed out.

The fourth paper is "*Unleashing Public-Key Cryptography in Wireless Sensor Networks*" by Javier Lopez. Sensor network technology has been shown to be of great value for a whole range of wireless applications. Representative security problems from typical wireless networks have needed much extra effort from researchers when facing the constrained nature of the sensor platforms and, in fact, other new and specific security issues still need to be worked out. This paper first overviews wireless sensor network (WSN) technology and applications. Then, it focuses on the security issues by analyzing the use of symmetric cryptography in contrast with public-key cryptography, and the important role that elliptic curve cryptography is playing in this field. Finally, it puts into perspective some important results obtained by different authors during the last couple of years and that all together demonstrate that there is an important place for public-key technology based solutions in WSN applications.

Guest Editors

Jianying Zhou
Institute for Infocomm Research, Singapore
E-mail: jyzhou@i2r.a-star.edu.sg

Meng-Chow Kang
Microsoft Asia Pacific, Singapore
E-mail: MengChow.Kang@microsoft.com