Journal of Computer Security 19 (2011) 227–228
DOI 10.3233/JCS-2010-0405
IOS Press

Guest editors' preface

In March 2010, the 2010 Workshop on RFID Security (RFIDSec'10 Asia) was held in Singapore, in which we served as program co-chairs. Aligned with the earliest RFID security workshop (RFIDsec) starting in 2005, this workshop provided an international forum for sharing original research results and application experiences among researchers in the field of RFID system security. The workshop was an overwhelming success, with twelve high-quality papers being included in the workshop program.

To further promote the fast-evolving research on RFID system security, we solicited original research papers in the theory and practice concerning RFID system security for a special issue in *Journal of Computer Security*. After rigorous review, this special issue selected two papers (after significant extensions) out of the twelve papers appeared in RFIDsec'10 Asia workshop and three papers out of fourteen new submissions after the workshop.

These five papers reflect different aspects of RFID system security, ranging from theoretical study on unconditionally secure approach for low-cost RFID systems to experimental research on practical eavesdropping and skimming attacks, from RFID distance-bounding protocols, secure ownership transfer of RFID tags to efficient construction of HB family protocols. A brief description of the subject matter is provided below.

While computationally secure protocols have been extensively studied in RFID system security research, the topic of unconditionally secure approach has been relatively neglected mainly for practical reasons: such approach would be less efficient and more costly. The paper "Securing low-cost RFID systems: An unconditionally secure approach", by Basel Alomair, Loukas Lazos and Radha Poovendran, seeks to bring more research to the design of unconditionally secure protocols that are suitable for low-cost RFID tags with stringent computational capabilities. The key idea in their work is to let RFID readers, which are computationally powerful, generate random numbers and deliver them to RFID tags in an unconditionally secure manner, after which an unconditionally secure message authentication code can be computed with a single multiplication operation on the tag side so as to solve the identity authentication problem in RFID systems.

"Practical eavesdropping and skimming attacks on high-frequency RFID tokens", by Gerhard P. Hancke, adds to our understanding of the feasibility of practical attacks against standard high-frequency RFID tokens. The major contribution of this paper is to provide enough details about experimental setup and results for eavesdropping and skimming attacks to high-frequency RFID tokens, confirming that near-field RFID devices are vulnerable to practical attacks beyond the advertised operating range.

Motivated by an observation that RFID distance bounding protocols are commonly designed without any formal approach, Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardaş, Cédric Lauradoux and Benjamin Martin, in “A framework for analyzing RFID distance bounding protocols”, provide a unified framework for analyzing distance bounding protocols. Their framework consists of a thorough analysis of the terminology in distance bounding domain, a generic and precise model for an adversary's capabilities and strategies, and a new view on the impact of the prover's ability to tamper with his/her devices. The paper also illustrates how the proposed framework allows refining the security analysis of an existing distance bounding protocol.

Secure ownership transfer of RFID tags is a critical issue in many RFID applications involving multiple parties. Several security properties have been identified in previous research on this subject, including controlled delegation, previous owner privacy, new owner privacy and temporary authorization recovery. This paper further identifies four new security properties that are equally important for practical ownership transfer, which are tag assurance, undeniable ownership transfer, current ownership proof and owner initiation. The paper also proposes a new RFID ownership transfer scheme that satisfies the desired security properties.

Tzipora Halevi, Nitesh Saxena and Shai Halevi, in “Tree-based HB protocols for privacy-preserving authentication of RFID tags”, address the challenges in combining traditional HB-like protocols with tree-based approaches. Traditional HB-like protocols are suitable for low-cost RFID tags due to simple operations performed on the tag side; however, an exhaustive search of RFID tags on the reader side is not scalable, and it may lead to a high false accept rate. On the other hand, traditional tree-based approaches require RFID tags to perform PRF operations, and therefore not applicable to very-low-cost tags. This paper proposes a “hybrid” solution that consists of two stages: in the first stage, the reader identifies the most likely tag to authenticate in a tree structure; in the second stage, the identity of the most likely tag is verified in a HB-like procedure. The proposed solution is suitable for low-cost tags and is optimized in terms of computation, communication and memory overheads.

Yingjiu Li
School of Information Systems
Singapore Management University

Jianying Zhou
Institute for Infocomm Research, Singapore