Journal of Computer Security 19 (2011) 1027–1028
DOI 10.3233/JCS-2011-0441
IOS Press

Guest Editor's Preface

This Special Issue is based on original research ideas, which were initially expressed in papers published in the *Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS-2010)*. ESORICS-2010 was held on September 2010 in Athens, Greece. The symposium has a tradition that goes back for two decades. It brings together the international research community in a top quality event that covers all the areas of computer security, ranging from theory to applications. ESORICS-2010 received 201 submissions, which went through a careful review process. As a result of this process, 42 papers were selected for the final program (21% acceptance rate).

To further promote the fast-evolving research in security, a few research papers were selected, among those published in the proceedings of ESORICS-2010, for a Special Issue in the *Journal of Computer Security*. These papers were significantly extended and went through another rigorous review. As a result, the Special Issue finally includes four papers. The papers reflect different aspects of security, ranging from RFID privacy and PKI-based systems, to information flow, and the IO2BO threat. A brief description of them is provided below.

In their paper, entitled "On bounding problems of quantitative information flow", H. Yasuoka and T. Terauchi investigate the hardness of precisely checking the quantitative information flow of a program. More precisely, the authors study the "bounding problem" of quantitative information flow, defined as follows: Given a program M and a positive real number q, decide if the quantitative information flow of M is less than or equal to q. Authors prove that the bounding problem is not a k-safety property for any k (even when q is fixed, for the Shannon-entropy-based definition with the uniform distribution), and thus is not amenable to the self-composition technique that has been successfully applied to checking non-interference. They also prove complexity theoretic hardness results for the case when the program is restricted to loop-free Boolean programs.

C. Zhang, T. Wang, T. Wei, Y. Chen and W. Zou, in their paper, entitled "Using type analysis in compiler to mitigate integer-overflow-to-buffer-overflow threat", deal with one of the top two causes of software vulnerabilities in operating systems, i.e., the integer overflow and, in specific, the Integer Overflow to Buffer Overflow (IO2BO) vulnerability. Authors present the design and implementation of IntPatch, a compiler extension for automatically fixing IO2BO vulnerabilities in C/C++ programs at compile time. IntPatch utilizes classic type theory and a dataflow analysis framework to identify potential IO2BO vulnerabilities. Then uses backward slicing to find out related vulnerable arithmetic operations and instruments programs with runtime checks. Authors, finally, evaluate IntPatch on a number of real-world applications.

Research on specific open RFID issues is the aim of the next two papers. R. Deng, Y. Li, M. Yung and Y. Zhao, in their paper, entitled "A zero-knowledge based framework for RFID privacy", develop a definitional framework for RFID privacy. The framework is based on a zero-knowledge formulation and incorporates the notions of adaptive completeness and mutual authentication. They provide meticulous justification of the new framework and contrast it with existing ones in the literature. They prove that their framework is strictly stronger than the ind-privacy model, which answers an open question for developing stronger RFID privacy models. They also clarify certain confusions and rectify several defects in the existing frameworks. Finally, they propose an efficient RFID mutual authentication protocol and analyze its security and privacy.

R. Nithyanand, G. Tsudik and E. Uzun, in their paper, entitled "User-aided reader revocation in PKI-based RFID systems", argue that a current prominent challenge is how to handle revocation and expiration checking of RFID reader certificates. This is an important issue considering that these high-end RFID tags are geared for applications such as e-documents and contactless payment instruments. Furthermore, the problem is unique to public key-based RFID systems, since a passive RFID tag has no clock and thus cannot use time-based on-line methods. The authors address the problem of reader certificate expiration and revocation in PKI-based RFID systems. They observe an important distinguishing feature of personal RFID tags used in authentication, access control or payment applications – the involvement of a human user. Then, they take advantage of the user's awareness and presence to construct a simple, efficient, secure and feasible solution. Finally, they evaluate the usability and practical security of their solution via user studies and discuss its feasibility.

I hope that the papers in this Special Issue can help the reader with her/his research and professional activities, and serve her/him as a source of inspiration during the difficult but fascinating route towards an on-line world with adequate security.

Prof. Dimitris Gritzalis
Department of Informatics
Athens University of Economics and Business