Electronic Commerce Research (2019) 19:471–475
https://doi.org/10.1007/s10660-019-09365-4

Editorial: special issue on advances in security and privacy for future mobile communications

Georgios Kambourakis · Gregorio Martínez · Felix Gómez Mármol

Published online: 17 July 2019

1 Introduction

Without doubt, the advances in wireless communication technologies like 3G, WiFi, WiMax and the proliferation of mobile devices have enabled the realization of pervasive and intelligent environments for users to communicate with each other, interact with information processing devices, and acquire ubiquitously a plethora of mobile services through various types of wireless access networks. Under this prism, reliable, secure, and privacy preserving communications combined with constant and universal network availability are vital elements for the adoption of any application that utilize wireless technologies. This becomes even more apparent when considering the tight coupling of these wireless network domains to the Internet. Every day new security challenges come to the surface due to the open nature of the wireless medium, the dynamic network topology, the resource constraints of the mobile devices and, in some cases, the lack of a pre-deployed infrastructure.

This special issue aims to advance state-of-the-art research in the area of security, privacy, cryptography, and its applications for future mobile communications. In this context, it addresses all aspects of the modeling, designing, implementation, assess-

G. Kambourakis (✉)
Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece
e-mail: gkamb@aegean.gr

G. Martínez
Department of Information and Communications Engineering, University of Murcia, Murcia, Spain
e-mail: gregorio@um.es

F. Gómez Mármol
NEC Laboratories Europe, Heidelberg, Germany
e-mail: felix.gomez-marmol@neclab.eu

ment, deployment and management of mobile network security and privacy systems, protocols and architectures. Also, the issue at hand pays particular attention to contributions devoted to secure and privacy preserving applications and services in the mobile ecosystem. The special issue is composed of seven refereed papers covering such topics as anonymous RA for trusted computing, cooperative security system for m-Health applications, a security solution for the IMS media plane, a comprehensive survey on Anonymous Voice over IP (VoIP) communication, an untraceable authentication method for large-scale active-tag RFID systems, and so forth. It is expected that the special issue will stimulate further related research and technology improvements in this significant and appealing subject.

2 Papers in this special issue

The first manuscript, "A Survey on Anonymous Voice over IP Communication: Attacks and Defenses" by Ge Zhang and Simone Fischer-Hübner, provides an up-to-date comprehensive survey on anonymous VoIP communication, considering both attacks and defenses. Today, VoIP communications are important for many categories of users, such as journalists, human rights workers and the military. This is confirmed by recent research work showing an increasing interest in methods of anonymous VoIP communication. This survey starts by introducing and identifying the major concepts and challenges in this field. Then the authors review anonymity attacks on VoIP and the existing work done to design defending strategies. Finally, they propose a taxonomy of attacks and defenses and discuss possible directions for future work in this continuously evolving field.

In the second paper, entitled "All-or-nothing approach to protect a distance bounding protocol against terrorist fraud attack for low-cost devices" by Abolfazl Falahati and Hoda Jannati, authors deploy an all-or-nothing method towards proposing a new distance bounding protocol with higher security level that is able to prevent terrorist fraud attack performed over the existing distance bounding protocols. According to the authors, their proposal is the first distance bounding protocol which can overcome all the three fraud attacks, namely mafia fraud, distance fraud and terrorist fraud simultaneously, showing at the same time the lowest success probability of the attacks compared with the well known distance bounding protocols. Moreover, the authors' proposal can be implemented using a low-cost device due to low computational cost and minimum system memory requirements.

The third paper, by Yalin Chen and Jue-Sam Chou, entitled "ECC-Based Untraceable Authentication for Large-Scale Active-Tag RFID Systems", focuses on elliptic-curve-cryptography (ECC)-based full-fledged RFID authentication protocols. The authors observe that some of these protocols violate location privacy or suffer from man-in-the-middle issues, while others generate excessive communication costs requiring at least three passes of message transmission between the tag and the back-end server. Compelled by these shortcomings, the authors construct two novel ECC-based two-pass RFID authentication protocols, namely PI and PII. The first one is designed for secure environments and is suitable for applications, including e-Passport and toll payment in vehicular ad-hoc networks. The latter is destined to hostile environ-

ments and can be applied in pseudonymous payment or anti-counterfeiting services. They conclude that PII is able to resist many attacks, outperforms previous ECC-based proposals in communication efficiency, and provides mutual authentication function and scalability.

The fourth contribution, "An Efficient Anonymous Remote Attestation Scheme for Trusted Computing based on Improved CPK" by Yu Fajiang, Chen Jing, Xiang Yang, Zhu Jiacheng and Zhao Yangdi, concentrates on platform remote attestation (RA) as one of the main features of trusted computing platform (TCP). The authors propose a RA scheme for TCP, namely RA-ICPK, based on an improved combined public key cryptography (ICPK). In fact, RA-ICPK is a certificate-less scheme, which combines commitment scheme, zero-knowledge proof and ring signature to own the security property of unforgeability and privacy while maintaining high efficiency. RA-ICPK is mainly based on elliptic curve cryptography, and only carries out zero-knowledge proof once. RA-ICPK does not depend on trusted third parties to check trusted platform module's (TPM) identity and integrity metrics revocations. RA-ICPK can help to reduce the users' economic burden and promote the development of trusted computing.

In the fifth paper, "Securing Coalitional Game for Distributed Cooperative Spectrum Sensing in Multi-channel Cognitive Radio Networks", authored by Behzad Kasiri, Jun Cai and Attahiru S. Alfa, a secure scheme for coalitional game in multi-channel cognitive radio networks is proposed. First, a distributed cooperative attack on multi-channel cooperative spectrum sensing is analyzed. Specifically, attackers play two coalitional games to maximize the number of invaded channels in a distributed manner. In the first game, attackers play with their fellow ones to allocate an optimal number of attackers for each channel, while in the second, they play in the coalitions with other honest cognitive radios so as to conquer as many channels as possible. Next, a hierarchical ID-based key management scheme is proposed, where cognitive radios can only play on a certain number of requested channels. Also, channel access for sensing is limited to the honest cognitive radios selected in the coalitional game. Simulation results show that the studied attack is able to significantly decrease the number of potential channels with a low attack cost when security scheme is not considered, in addition to the energy efficiency of the proposed key management scheme. The authors also provide a formal verification of the proposed key management scheme.

The sixth manuscript, entitled "Towards a Cooperative Security System for Mobile-Health Applications", by Bruno M. C. Silva, Joel J. P. C. Rodrigues, Fábio Canelo, Ivo M. C. Lopes and Jaime Lloret, offers a novel data encryption solution for mobile health systems, considering a new and early-proposed cooperation strategy. This encryption solution, called data encryption for mobile health applications (DE4MHA), attempts to guarantee the best confidentiality, integrity, and authenticity of users' data of m-health systems. The authors also present a performance evaluation study comparing the performance of an m-Health application with and without the DE4MHA.

The last contribution, "End-to-middle-to-end solution for IMS media plane security", authored by Jose Oscar Fajardo, Fidel Liberal, Fudong Li, Nathan Clarke and Is-Haka Mkwawa focuses on IP multimedia subsystem (IMS) security. The authors observe that the review of recent IMS security activities stresses the inclusion of intermediate nodes in the media path of secured communications as an open issue.

In this direction, they present an end-to-middle-to-end solution which enables the usage of IMS media plane elements such as recorders, transcoders and novel cross-ciphering functions in a secure way. The proposed solution, which is fully compliant with IMS, includes the network architecture, the signaling plane for session signaling and key management, and the media-plane security characteristics. Experimental results demonstrate that the proposed solution can provide media interoperability with a low cost of overhead to a standard IMS call setup in the signaling plane.

Acknowledgments The guest editors would like to express their thanks to Prof. Bezalel Gavish for giving the opportunity to edit this special issue on advances in security and privacy for future mobile communications, and Ms. Jackie James for making this issue published. Also, we wish to thank the authors for submitting their work as well as the tireless reviewers who have constructively evaluated the papers within the short stipulated time. Finally, we sincerely hope the reader will share our view and find this special issue very useful.

Georgios Kambourakis received the Diploma in Applied Informatics from the Athens University of Economics and Business and the Ph.D. in Information and Communication Systems Engineering from the dept. of Information and Communications Systems Engineering, University of the Aegean. He also holds a Master of Education degree from the Hellenic Open University. Currently, he is an Assistant Professor at the department of Information and Communication Systems Engineering, University of the Aegean, Greece. His research interests are in the fields of mobile and wireless networks security and privacy, VoIP security, PKI, DNS security, and mLearning and he has more than 85 publications in the above areas. He has been involved in several national and EU funded R&D projects in the areas of Information and Communication Systems Security. He is also a reviewer of several IEEE and other international journals and has served as a technical program committee member for more than 100 international conferences in security and networking.

Gregorio Martínez is Associate Professor in the Department of Information and Communications Engineering of the University of Murcia. His research interests include security and management of distributed communication networks. He received the M.Sc. and Ph.D. degrees in Computer Science from the University of Murcia. He has published more than a hundred journal articles and conference papers. He has been involved as collaborator or supervisor in several open-source software projects. He is also on the editorial or review board of more than 20 international journals.

Felix Gómez Mármol is a Senior Researcher in the Security Group at NEC Laboratories Europe, Heidelberg, Germany. His research interests include authorization, authentication and trust management in distributed and heterogeneous systems, security management in mobile devices and design and implementation of security solutions for mobile and heterogeneous environments. He published over 30 research articles, holds 4 patents and participated in several special issues as guest editor in international journals. He received an MSc and Ph.D. in computer engineering from the University of Murcia.