EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

EDITORIAL Open Access

Security and resilience for smart devices and applications

Damien Sauveron[1*], Konstantinos Markantonakis[2] and Christos Verikoukis[3]

Abstract

Recent advances in development of wireless communication technologies and embedded computing systems led us into the area of the next generation wireless networks and smart devices. In this context, it is widely argued that security has become a primary concern, in order to ensure dependable, secure communications and services to the end user. There are many open questions for these challenging issues such as security of protocols and applications, secure architecture, frameworks and methodologies for next generation wireless networks and respective smart devices.

This exciting special issue has received 78 submissions that covered all topics of security and resilience for smart devices and wireless networks. After a long, rigorous and highly competitive review process, only 20 papers have been accepted for publications. These papers are categorised in two groups, one related to smart device security and one related to wireless networks.

The first group of 7 papers describes various research works related to smart devices. The first paper, 'A secure and robust connectivity architecture for smart devices and applications' by Shon et al., presents a novel connectivity architecture using RF4CE-based wireless zero-configuration and enhanced key agreement approach which has been analysed further through mobile devices and a prototype hardware (H/W). The second and third papers are based on how SIM cards can be used to enhance the security of two different systems. Indeed, the second paper, 'A USIM-based uniform access authentication framework in mobile communication' by Li et al., proposes a uniform access authentication framework based on the EAP authentication protocol in order to add a media-independent authentication layer in USIM, along with a key adaptation layer (for terminals) which enables to meet the specific requirements of various communication modules. In the third paper, 'CS-DRM: a cloud-based SIM DRM scheme for mobile internet', Wang et al. introduce a SIM card into a Digital Rights Management (DRM) system to both reduce the cost of the servers in a DRM system when the number of users scales up and in turn provide higher security. The fourth and fifth papers relate to radio frequency identification (RFID) technology. In the fourth paper, 'Who counterfeited my Viagra?' Probabilistic item removal detection via RFID tag cooperation', Conti et al. provide a set of probabilistic protocols that detect the absence of a RFID tag from a system composed of a set of tags and a reader. In the fifth paper, 'A salient missing link in RFID security protocols', Erguler et al. demonstrate how timing attacks can be achieved on some well-known lightweight RFID security protocols. The aims of this paper are to jeopardize the system's untraceability criteria and to outline a countermeasure by precisely describing the database query mechanism. The sixth and seventh papers are dedicated to particular smart devices: smart camera and cognitive radio. The sixth paper, 'Securing embedded smart cameras with Trusted Computing' by Winkler et al., presents an embedded camera prototype that uses Trusted Computing to provide security guarantees for streamed videos. The seventh paper, 'Modeling the lion attack in cognitive radio networks' by Hernandez-Serrano, presents a cross-layer attack to Transmission Control Protocol (TCP) connections in cognitive radio networks, analyzes its impact on TCP throughput via analytical model and simulation and finally proposes potential countermeasures to mitigate it.

The second group is comprised of 13 research papers related to wireless networks. The first two papers consider privacy protection. In the first paper, 'HOP: achieving efficient anonymity in MANETs by combining HIP,

* Correspondence: damien.sauveron@unilim.fr
[1]University of Limoges, XLIM UMR CNRS, Limoges 87060, France
Full list of author information is available at the end of the article

OLSR, and pseudonyms', Campos et al. propose and implement a novel solution based on cryptographic Host Identity Protocol (HIP) that offers security and user-level anonymity in MANET environments while maintaining adequate performance levels. The second paper, 'Secure and efficient protocol for vehicular ad hoc network with privacy preservation' by Choi et al., presents a secure yet efficient protocol for a VANET that satisfies privacy and traceability requirements. The next two papers investigate energy efficient solutions. In the third paper, 'Energy-efficient source authentication for secure group communication with low-powered smart devices in hybrid wireless/satellite networks', Roy-Chowdhury et al. describe a new class of lightweight, symmetric-key digital certificates called extended TESLA certificates and a source authentication protocol for wireless group communication applied to a hybrid wireless network with a satellite overlay interconnecting the wireless devices. In the fourth paper, 'EDDK: energy-efficient distributed deterministic key management for wireless sensor networks', Zhang et al. present an energy-efficient distributed deterministic key management scheme (EDDK), based on elliptic curve cryptography (ECC) for resource-constrained wireless sensor networks (WSNs). The next five papers present various cryptographic key schemes. In the fifth paper, 'Broadcast secrecy via key-chain-based encryption in single-hop wireless sensor networks', Sivaraman et al. propose, implement and evaluate a scheme that meets the requirements of secrecy, authenticity, integrity and freshness of broadcast messages in the context of a single-hop wireless sensor network (WSN). In the sixth paper, 'Efficient public key certificate management for mobile ad hoc networks', Caballero-Gil et al. propose an efficient public key management scheme that is suitable for fully self-organized mobile ad hoc networks where all nodes serve identical roles. In the seventh paper, 'A family of key agreement mechanisms for mission critical communications for secure mobile ad hoc and wireless mesh internetworking', Askoxylakis et al. examine the attributes of each key establishment method and how each method can be better applied in different scenarios for both MANETs and mesh networks considering system and application requirements such as efficient and secure internetworking, dynamicity of network topologies and support of thin clients. In the eighth paper, 'Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks', Azarderskhsh et al. propose a secure clustering scheme along with a deterministic pairwise key management scheme based on public key cryptography to address security issues in the heterogeneous WSNs. In the ninth paper, 'A forward authentication key management scheme for heterogeneous sensor networks', Huang et al. propose a new key management method that uses dynamic key management schemes for heterogeneous WSNs. Then, in the tenth paper, 'Efficient key agreements in dynamic multicast height balanced tree for secure multicast communications in ad hoc networks', Lin et al. propose a dynamic multicast height balanced group key agreement (DMHBGKA) that allows a user in a multicast group to efficiently and dynamically compose the group key and securely deliver multicast data from a multicast source to the other multicast group users in wireless ad hoc networks. The last three papers investigate various topics related to security in wireless networks.

The eleventh paper, 'Secure Rateless Deluge: pollution-resistant reprogramming and data dissemination for wireless sensor networks' by Law et al., proposes a secure version of Rateless Deluge that is resistant to pollution attacks. Sreluge employs a neighbour classification system and a time series forecasting technique to isolate polluters and a combinatorial technique to decode data packets in the presence of polluters before the isolation is complete. The twelfth paper, 'Wireless Information-Theoretic Security in an outdoor topology with obstacles: theoretical analysis and experimental measurements' by Chrysikos et al., presents a Wireless Information-Theoretic Security scheme, which has been recently introduced as a robust physical layer-based security solution, especially for infrastructureless networks. Finally, the thirteenth paper, 'A wireless sensor network for hospital security: from user requirements to pilot deployment' by Kaseva et al., presents a novel WSN design targeted at applications requiring low data transfer delays and high reliability and the whole design flow from user requirements to an actual pilot deployment in a real hospital unit.

Acknowledgements

We would like to thank all the authors who have submitted their papers. We would also like to thank all the reviewers for their time and efforts. Their thorough reviews and valuable comments helped us to select the papers, as well as improve the quality of this special issue. However, special thanks go to Professor Luc Vandendorpe, Editor-in-Chief, for approving and making this issue possible and to the staff of EURASIP Journal on Wireless Communications and Networks for their priceless and constant support along the whole process. Finally, we hope that the contents of this special issue will serve as good references for your research work. This special issue has been partially supported by the research projects Network of Excellence NEWCOM++ (FP7-ICT-216715), COOLNESS (FP7-IAPP-218163) and CO2GREEN (TEC2010-20823) through the involvement of C. Verikoukis in the editorial activities.

Author details

[1]University of Limoges, XLIM UMR CNRS, Limoges 87060, France. [2]Information Security Group, Royal Holloway, University of London, Surrey TW20 0EX, UK. [3]Telecommunications Technological Centre of Catalonia, Castelldefels 08860, Spain.

Received: 17 June 2014 Accepted: 10 July 2014
Published: 29 July 2014

doi:10.1186/1687-1499-2014-123
Cite this article as: Sauveron *et al.*: Security and resilience for smart devices and applications. *EURASIP Journal on Wireless Communications and Networking* 2014 **2014**:123.