Mobile Networks and Applications (2020) 25:151–152
https://doi.org/10.1007/s11036-019-01438-w

Editorial: Security and Privacy Protection for Mobile Applications and Platforms

Victor Sucasas[1] · Georgios Mantas[2] · Saud Althunibat[3] · José-Fernán Martínez Ortega[4]

Published online: 3 January 2020

Editorial:

Mobile networks and applications are currently developing at a rapid pace due to the increasing relevance of mobile IoT in strategic scenarios such as Smart Cities, Intelligent Transportation and Industry 4.0. Novel digital technologies will enable cities and industry to streamline their infrastructures, which will improve the inhabitants' well-being, boost their production processes, and provide efficient and scalable logistics while maintaining the ever increasing demand for green and eco-friendly technological standards. However, this rapid growth of distributed connected mobile systems will pose a challenge on how to protect mobile devices and preserve the privacy of the users. Preventing malware attacks, remote hijacking, DDoS attacks, or traffic analysis and user profiling will be of paramount importance to protect applications and platforms functionality and preserve user privacy. This special issue focuses on novel security and privacy solutions for mobile applications and platforms addressing the important challenges in the Smart City scenario and presenting novel research or experimental results. The selected papers focus on different topics covered under the umbrella of Smart City concept such as: Lightweight security mechanisms for IoT; Blockchain-based IoT security; Physical-layer security; Security and privacy for mobile devices; Cybersecurity for Cyber Physical Production Systems (CPPSs); among others.

This special issue features seven selected papers with high quality. The first article, "Reliable Data Analysis through Blockchain based Crowdsourcing in Mobile Ad-hoc Cloud", authored by Saqib Rasool, proposed a blockchain based reputation system for detection of malicious nodes in crowdsourcing, and provides a comprehensive analysis of this technical challenge together with experimental results of the proposed approach.

The second article titled "An Autonomous Host-based Intrusion Detection System for Android Mobile Devices", authored by Jose Ribeiro, presented a novel approach based on machine learning and statistical analysis for the detection of malicious software in mobile devices, and caters for its Android implementation. In the fourth article, "AdDroid: Rule based Machine Learning Framework for Android Malware Analysis" also focuses on the same problem of malware detection and propose machine learning leveraged by feature selection and extraction techniques to improve performance, with a low-complex implementation that enables real-time analysis.

In the third article with the title "A Physical-Layer Key Distribution Mechanism for IoT Networks", the authors focus on constrained IoT networks and propose physical layer security as a lightweight approach for key distribution mechanisms. Although physical layer security has been widely studied as a lightweight approach to transmit confidential information, authors in this article propose physical layer security for symmetric key agreement between multiple entities. In the fifth article, "Secrecy Performance in the Internet of Things: Optimal Energy Harvesting Time Under Constraints of Sensors and Eavesdroppers", authors also focus on physical layer security for IoT networks, namely wireless sensor networks powered with energy harvesting technologies. This paper focuses on the wireless communication between power transfer units and sensing nodes, and the influence of passive attacks performed by malicious nodes eavesdropping the communications.

The articles "Cryptanalysis of Merkle-Hellman cipher using parallel genetic algorithm", authored by Nedjmeddine Kantour

✉ Victor Sucasas
vsucasas@ua.pt

Georgios Mantas
gimantas@av.it.pt

Saud Althunibat
saud.althunibat@ahu.edu.jo

José-Fernán Martínez Ortega
jf.martinez@upm.es

[1] Universidade de Aveiro, 3810-193 Aveiro, Portugal

[2] Instituto de Telecomunicações, University of Aveiro, 3810-193 Aveiro, Portugal

[3] Al-Hussein Bin Talal University, Ma'an, Jordan

[4] Universidad Politécnica de Madrid, 28040 Madrid, Spain

and "IBEET-RSA: Identity-Based Encryption with Equality Test over RSA for Wireless Body Area Network" by Mohammed Ramadan provide novel cryptographic schemes to enable data confidentiality using public key cryptography and identity-based cryptography respectively.

Acknowledgements The guest editors are thankful to our reviewers for their effort in reviewing the manuscripts. We also thank the Edit-in-Chief, Dr. Imrich Chlamtac for his supportive guidance during the entire process. The special issue is sponsored by BROADNETS 2018 conference and the i-Five (POCI-01-0145-FEDER-030500, funded by FEDER, through COMPETE 2020, Regional Operational Program of the Algarve 2020 and Fundação para a Ciência e Tecnologia) and SECRET (H2020-MSCA-ITN-2016 SECRET-722424) projects.

Victor Sucasas obtained his Ph.D. on Electrical and Electronic Engineering at University of Surrey (UK) in 2016. He has extensive research experience as a researcher at Instituto de Telecomunicaçõs - Aveiro, Portugal and at University of Surrey, Guildford, UK, where he worked on European projects FP7-GREENET, ECSEL-SWARMs, CATRENE-H2O and ECSEL-SECREDAS. Since 2016, he has been a senior researcher at University of Aveiro in network security and privacy preserving systems. His research interests cover privacy-preserving authentication mechanisms, pseudonymization and anonymization, eliptic curve cryptography and identity-based cryptography. He is and IEEE member and an EAI Fellow.

Georgios Mantas received the Diploma degree in electrical and computer engineering from the University of Patras, Greece, in 2005, the M.Sc. degree in information networking from Carnegie Mellon University, PA, USA, in 2008, and the Ph.D. degree in electrical and computer engineering from the University of Patras, in 2012.,In 2014, he became a Postdoctoral Researcher at the Instituto de Telecomunicações, Aveiro, Portugal, where he has been involved in research projects, such as ECSEL—SemI40, CATRENE—MobiTrust, CATRENE—NewP@ss, ARTEMIS—ACCUS, FP7—CODELANCE, and FP7—SEC-SALUS. Since 2018, he has been a Lecturer with the University of Greenwich, U.K. His main research interests include network and system security, authentication mechanisms, privacy-preserving mechanisms, intrusion detection systems, and secure network coding.

Saud Althunibat received the Ph.D. degree in telecommunications from the University of Trento, Italy, in 2014. He is currently an Assistant Professor with Al-Hussein Bin Talal University, Jordan. He has authored more than 60 scientific papers. His research interests include index modulation, physical-layer security, spectrum sharing, cognitive radio, wireless sensor networks, and energy efficiency and resource allocation. He served as a General Co-Chair of BROADNETs 2018 conference. (Based on document published on 4 April 2019).

José-Fernán Martínez Ortega received the Ph.D. degree in telematic engineering from the Technical University of Madrid, Madrid, Spain, in 2001, where he is currently an Associate Professor with the Department of Engineering and Telematic Architectures.,He is responsible for different Spanish and European public-funded research projects and also research contracts with different IT companies. His main research interests include ubiquitous computing and the Internet of Things, smart cities and wireless sensor and actuators networks, next-generation telematic network and services, software engineering and architectures, distributed applications and intermediation platforms (middleware), and high-performance and fault-tolerant systems. He has authored several national and international publications included in the Science Citation Index in his interest areas. He has participated in several international and European projects.,Dr. Martínez is a Technical Reviser and the Chair of technical national and international events on telematics and a member of different international and scientific committees.