de Fuentes, J.M., Gonzalez-Manzano, L., Lopez, J. et al. Editorial: Security and Privacy in Internet of Things. *Mobile Netw Appl* **24**, 878–880 (2019).

DOI: 10.1007/s11036-018-1150-8

Editorial: Security and Privacy in Internet of Things

Jose M. de Fuentes[1] • Lorena Gonzalez-Manzano[1] • Javier Lopez[2] • Pedro Peris-Lopez[1] • Kim-Kwang Raymond Choo[3]

1 Editorial

In our daily life, we interact with a large number of variety of technological devices for difference purposes, such as accessing documents stored in the cloud, viewing photos and videos, and remotely controlling devices in a smart home. Many of these devices are also Internet-connected, and hence they are also commonly referred to as Internet of Things (IoT).

There is a broad range of use cases for IoT, ranging from the healthcare sector (e.g. remote monitoring and collection of body and health-related information) to a smart city environment (e.g. vehicular ad hoc networks – VANETs, to facilitate safety-related, traffic management or infotainment services) to a more adversarial environment (e.g. battlefields).

There are, however, a number of challenges to be addressed in any IoT deployment, and two of these key challenges are security and privacy, particularly as the data from IoT devices are being sent and shared via some remote cloud services. The critical nature of some of these IoT applications (medical, battlefield, etc.) also call for development of tailored approaches.

Therefore, in this Special Issue, novel security and privacy approaches are presented in the six accepted articles.

The first article entitled 'Crowdsourcing analysis in 5G IoT: Cybersecurity Threats and Mitigation' by Ana Nieto, Antonio Acien and Gerardo Fernandez, studies security threats in IoT ecosystem, and seeks to mitigate such risks leveraging 5G technology [3].

[1] Jose M. de Fuentes
jfuentes@inf.uc3m.es
Lorena Gonzalez-Manzano
lgmanzan@inf.uc3m.es
Pedro Peris-Lopez
pperis@inf.uc3m.es
[2] Javier Lopez
jlm@lcc.uma.es
[3] Kim-Kwang Raymond Choo
raymond.choo@fulbrightmail.org
1 Computer Security Lab (COSEC). Computer Science and Engineering Department, Universidad Carlos III de Madrid, Madrid, Spain
2 Universidad de Malaga, Malaga, Spain ´
3 University of Texas at San Antonio, San Antonio, TX 78249, USA

In particular, the authors demonstrate how crowdsourcing techniques (i.e. cooperative approaches in which participants are rewarded for their participation) could be applied to this context. They identify several several use cases, such as information sharing among service providers and the implementation of digital witnesses in such an environment environment. They also propose a model to implement the presented approach and illustrate the effect of crowdsourcing in an attack to a VoIP system.

The second article, 'Identity-based user authenticated key agreement protocol for multi-server environment with anonymity', by Alzubair Hassan, Anyembe Andrew Omala, Mohamed Ali, Chunhua Jin and Fagen Li, focuses on IoT scenarios in which several servers co-exist and a single registration are desired [1]. Existing proposals are limited in that once credentials are stolen from one service, the remaining ones might be under the control of the attacker. To overcome this limitation, the authors propose an identitybased user authenticated key agreement scheme, which provides unconditional anonymity. Their ring signaturebased approach is proven secure, and its performance evaluated on an Android device. Their results show that achieving this higher degree of privacy comes at the cost of increased computation and communication costs.

Another typical scenario for IoT devices, namely Mobile Ad-Hoc Networks (MANETs), is the context of the third contribution. In 'Determining the honesty of the accuser node in key revocation procedure for MANET', Maryam Zarezadeh and Hamid Mala focus on assessing the legitimacy of the nodes t[4]hat cooperate in a key revocation process [6]. Once an IoT device is found to be compromised or misbehaving, it is important to evict it from the network. For this purpose, several existing schemes rely upon the opinion of other peer nodes. The proposal presented in their paper aims to determine how to set a statistical threshold to admit or reject accusations. Their performance results, based on simulations, show the time improvement as compared to previous schemes under different settings.

The fourth contribution, by Pradip Kumar Sharma, Jin Ho Park, Young-Sik Jeong and Jong Hyuk Park, focuses on a trending application of IoT – smart homes. In particular, authors explore how to apply Software-Defined Networks (SDNs) to achieve security in this scenario. In their paper, 'SHSec: SDN based Secure Smart Home Network Architecture for Internet of Things', the authors propose a flexible architecture that can deal with current and future security threats that may appear due to the interaction of IoT devices from different manufacturers [5]. Since their evolution pace may lead to threats that cannot be foreseen, it is important to count on an agile mechanism to mitigate their effects. Therefore, in a software-defined networking (SDN) approach, the data layer and control layers are detached. This results in a fast reaction against unexpected events. Different use cases are simulated to attest the accuracy and sensitivity of their system in detecting security events as well as the overhead incurred.

In the fifth paper, Sebastian Pape and Kai Rannenberg address privacy issues in a setting that is closely related to IoT – fog computing. In particular, their paper 'Applying Privacy Patterns to the Internet of Things' (IoT) Architecture' discusses how privacy patterns can be applied in this field [4]. Privacy patterns can be regarded as the means to turn the privacy-by-design principle in a real software implementation. Although many previous contributions have already addressed the problem of how to provide privacy in IoT, the aim of their paper is to identify which issues of this ecosystem can be leveraged to achieve privacy preservation. To show the application of their proposal, a smart vehicle scenario is analyzed.

Last but not least, the sixth paper, 'Decentralised functional signatures' by Bei Liang and Aikaterini Mitrokotsa, deals with the practical feasibility of digital signatures in the IoT ecosystem [2]. In particular, they focus on a particular type called functional signatures, which can be used to provide an intrinsic access control mechanism. Since they allow users to sign a given transformation of data, this mechanism prevents unauthorized access to the data itself. In order to make this mechanism suitable to the IoT context, they propose a multi-authority variant. Thus, different IoT devices (which may be issued or controlled by different authorities) can seamlessly cooperate. Their formal proofs show the theoretical validity of their proposal.

Acknowledgements. The guest editors are thankful to our reviewers for their effort in reviewing the manuscripts. We also thank the Editorin-Chief, Prof. Imrich Chlamtac to encourage us to organize this special issue. Moreover, authors want to thank Ms. Dominika Belisova and Ms. Rolissa Atienza for their kind assistance during the whole process. J. M. de Fuentes, L. Gonzalez-Manzano and P. Peris-Lopez have been partially supported by MINECO grants TIN2013-46469-R and TIN2016-79095-C2-2-R, and CAM grant S2013/ICE-3095.

References

1. Hassan A, Omala A, Ali M, Jin C, Li F (2018) Identity-based user authenticated key agreement protocol for multi-server environment with anonymity. Mobile Networks and Applications

2. Liang B, Mitrokotsa A (2018) Decentralised functional signatures. Mobile Networks and Applications

3. Nieto A, Acien A, Fernandez G (2018) Crowdsourcing analysis in 5g iot: Cybersecurity threats and mitigation. Mobile Networks and Applications

4. Pape S, Rannenberg K (2018) Applying privacy patterns to the internet of things (iot) architecture. Mobile Networks and Applications

5. Sharma P, Park J, Jeong YS, Park JH (2018) Shsec:sdn based secure smart home network architecture for internet of things. Mobile Networks and Applications

6. Zarezadeh M, Mala H (2018) Determining the honesty of the accuser node in key revocation procedure for manet. Mobile Networks and Applications

Jose M. de Fuentes is Associate Professor at the Computer Science and Engineering Department at Universidad Carlos III de Madrid. He is Computer Scientist Engineer (2007) and received a PhD in computer science from Universidad Carlos III de Madrid (2012). His research interests are applied cryptography, continuous authentication and security and privacy issues in the Internet of Things. In these areas, he has co-authored more than 20 journal papers as well as more than 15 conference articles. He is an editorial board member of Wireless Networks journal.

Lorena Gonzalez-Manzano is visiting lecturer in the Computer Science and Engineering Department at Universidad Carlos III de Madrid. She is a Computer Scientist Engineer (2010) and received a PhD in computer science (2014) by Universidad Carlos III de Madrid. Her research interests include the Internet of Things and cloud computing security. She has published 20 journal papers as well as 14 conference papers. She is an editorial board member of Future Generation Computer Systems journal.

Javier Lopez is Full Professor at the University of Malaga. His research activities are mainly focused on network security, security protocols and critical information infrastructures, leading a number of national and international research projects in those areas, including projects in FP5, FP6, FP7 and H2020 European Programmes. Prof. Lopez is the Spanish representative in the IFIP Technical Committee 11 on Security and Protection in Information Systems. Also, he is Co-Editor in Chief of International Journal of Information Security (IJIS), and a member of the Editorial Boards of, amongst others, IEEE Wireless Communications, Computers & Security, IEEE Internet of Things Journal, Journal of Computer Security, and IET Information Security. In the past, he was Chair of the IFIP Working Group 11.11 on Trust Management and Chair of the ERCIM Working Group on Security and Trust Management.

Pedro Peris-Lopez is Associate Professor at the Department of Computer Science, Universidad Carlos III de Madrid, Spain. He holds a M.Sc. in Telecommunications Engineering (2004) and Ph.D. in Computer Science by Universidad Carlos III de Madrid (2008). His research interests are in the field of cybersecurity and e-health, digital forensics and hardware security. In these fields, he has published a large number of articles in specialized journals (48) and conference proceedings (44). His works have more than 3400 citations and his h-index is 27. For additional information see: http://www. lightweightcryptography.com/.

Kim-Kwang Raymond Choo received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA), and has a courtesy appointment at the University of South Australia. He serves on the editorial board of Computers & Electrical Engineering, Computers & Security, Cluster Computing, Digital Investigation, IEEE Access, IEEE Blockchain Newsletter, IEEE Cloud Computing, IEEE Communications Magazine, IEEE Transactions on Big Data, Future Generation Computer Systems, Journal of Network and Computer Applications, PLoS ONE, Soft Computing, etc. In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the

Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, an IEEE Senior Member, and an Honorary Commander of the 502nd Air Base Wing, Joint Base San Antonio-Fort Sam Houston.