Preface

Arcangelo Castiglione*

Department of Computer Science,
University of Salerno,
Via Giovanni Paolo II 132,
84084 Fisciano SA, Italy
Email: arcastiglione@unisa.it
*Corresponding author

Xinyi Huang

College of Mathematics and Informatics,
Fujian Normal University,
No.1 Keji Road, Shangjie, Minhou,
Fuzhou, Fujian, 350117, China
Email: xyhuang@fjnu.edu.cn

Laurence T. Yang

St. Francis Xavier University,
4130 University Ave.,
Antigonish, NS B2G 2W5, Canada
Email: ltyang@stfx.ca

Alessio Merlo

Department of Informatics, Bioengineering, and Robotics,
University of Genoa,
Via Balbi, 5, 16126 Genova GE, Italy
Email: alessio.merlo@unige.it

Biographical notes: Arcangelo Castiglione received his MS and PhD in Computer Science from the University of Salerno, Italy. Currently, he is an Assistant Professor at the Department of Computer Science, University of Salerno (Italy). His research mainly focuses on cryptography, information security, computer security, and digital watermarking. He is an Associate Editor for the *IET Cyber-Physical Systems: Theory & Applications*, *Journal of High Speed Networks*, *International Journal of Embedded Systems*, *Future Internet*, *Bulletin of Electrical Engineering and Informatics* and *Connection Science*, and he has also been Guest Editor for several special issues and Volume Editor for *Lecture Notes in Computer Science*. He has been a member of several program committees for international conferences, and reviewer for several scientific journals and conferences. He serves as secretary the IEEE Technical Committee on Scalable Computing and the IEEE Systems, Man, and Cybernetics Technical Committee of Cybermatics.

Xinyi Huang received his PhD from the University of Wollongong, Wollongong, NSW, Australia. Currently, he is a Professor at the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China, and the Co-Director of the Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou. His current research interests include applied cryptography and network security. He is an Associate Editor of the *IEEE Transactions on Dependable and Secure Computing*. He serves on the Editorial Board for the *International Journal of Information Security* (Springer) and has served as the Program/General Chair or a Program Committee member in over 80 international conferences.

Laurence T. Yang is a Professor at the School of Computer Science and Technology of Huazhong University of Science and Technology and St. Francis Xavier University. He graduated from Tsinghua University and received his PhD from the University of Victoria, Canada. His current research includes parallel and distributed computing, and embedded and ubiquitous computing.

Alessio Merlo is an Assistant Professor in the Department of Informatics, Bioengineering, and Robotics at the University of Genoa. His research interests include performance and security issues related to the web, distributed systems (grid, cloud), and mobile devices. He received an MSc and PhD in Computer Science from the University of Genoa in 2005 and 2010,

respectively. He is on the editorial board of the *Journal of High Speed Networks* and has been a member of program committees for international conferences, including IFIP-SEC, AINA, ARES, and HPCS.

While conventional security and privacy techniques work well on systems that have acceptable computational and memory capabilities, this does not apply to the modern, pervasively interconnected world. Today there are multiple embedded systems and sensor networks with minimal computational and memory capabilities. Such systems and networks are closely linked to sensitive infrastructures and strategic services, such as the distribution of water and electricity, so designing and implementing privacy and security technologies in such environments is fundamental.

The introduction of lightweight techniques is essential to overcoming many of the problems arising from general security and privacy issues, such as constraints related to physical size, processing requirements, memory limitation and energy drain.

The main aim of this special issue has been to present innovative research contributions aimed at addressing security and privacy issues within modern constrained network environments and providing a bridge for discussions and opportunities between the academic and industrial worlds.

The issue will carry revised and substantially extended versions of selected papers presented at the 10th International Symposium on Cyberspace Safety and Security (CSS 2018), but we are also inviting other experts to submit articles for this call.

Among the around 21 submissions, just seven have been accepted for publication. The evaluation process of the submissions has been made rigorously, by professionals coming from several sectors, including both academia and industry.

The first contribution, co-authored by De Prisco et al., is entitled ‘Design of an outdoor position certification authority’. It proposes the design of an outdoor position certification authority. Such an authority aims at certifying the geolocalisation of a mobile device equipped with a global navigation satellite system receiver. Such a receiver is capable of acquiring radio signals (low-level data) and navigation messages (high-level data) in outdoor environments coming from different constellations of global/regional satellite navigation systems and satellite-based augmentation systems. To date, this information is unreliable from a security point of view because malicious attackers can easily forge it through specialised spoofing techniques. An outdoor position certification authority defines a client/server architecture through which a user can certify his position by sending the geolocalisation information needed to verify it to one or more remote servers. There are several scenarios for which this service can be handy, and with the advent of the internet of things, age devices that might require such a service will grow in number.

Recent technological advancements in the field of communication and control are transforming the transportation industry by extending the capabilities of conventional human-controlled vehicles to partially or fully automated vehicles. These vehicles create a network, also termed as internet of automated vehicles (IAV), having the capability of sensing the data from the surroundings and using it as a feedback mechanism in order to assist drivers and the static infrastructure for safe navigation and control. However, a uniform framework is required to isolate the interactions among the vehicles and different entities for secure transmission and control. In the article ‘Decentralised control-based interaction framework for secure data transmission in the internet of automated vehicles’, co-authored by Gupta and Quamara, the authors propose a decentralised control based interaction framework for promoting the smooth transmission of sensor data in the automated vehicular system and verify the correctness of the underlying policy model on the access control policy testing (ACPT) tool. Besides, the authors present some case studies to show the effectiveness of the proposed framework in real-time applications.

The resolution of video cameras has increased considerably in recent years. This fact has led to new generation video formats, with new compression methods and more sophisticated algorithms. However, compression can heavily affect the noise present in each frame, and encoder specific features can flatten the residual noise in the frame. In the article ‘An experimental estimate of the impact produced on PNU by new generation video codecs’, co-authored by Bruno and Cattaneo, the authors propose some experiments to verify whether the well-documented techniques for source camera identification based on PNU can still be applied to videos in these formats. Such experiments allowed the authors to build a fair input dataset without any hidden side-effects produced by the codecs and the post-processing tools installed on the device by the manufacturers.

In the article ‘Lightweight and efficient approach for multi-secret steganography’, co-authored by Koptyra and Ogiela, the authors compare the efficiency of two approaches for multi-secret steganography in lightweight systems: interlacing and multi-level. The study was conducted for two and three secrets with the use of the F5 algorithm for both approaches. The embedding times were measured with and without I/O operations. Finally, the application of these techniques in lightweight solutions is discussed.

Keyloggers and screenloggers are one of the active growing threats to user’s confidentiality as they can run in user-space, are easily distributed, and upload information to remote servers. They use a vast number of different technologies and may be implemented in many ways.

Keyloggers and screenloggers are easily diverted from their primary and legitimate function to be exploited for malicious purposes, compromising the privacy of users, and bank customers notably. Owing to the recent multiplication of mobile devices with a touchscreen, the screenlogger threat has become even more dangerous. This threat is even harder to fight, given the limited resources of the affected devices. In the article 'A survey on screenlogger attacks as well as countermeasures', co-authored by Sbai et al., the authors take the first step of a project aiming at proposing efficient countermeasures against screenloggers. It provides a complete overview of the different techniques used by this malware and discusses an extensive set of plausible countermeasures.

Different steganography techniques have been presented based on the RGB image, as the image is considered a secure cover for hidden data. In the article, 'Secure RGB image steganography based on modified LSB substitution', authored by Almazaydeh, the author presents an edge-based image steganographic method that relies on embedding the secret message bits into variable LSB length of the blue colour channel of the cover image. The blue colour channel is selected because the steganography-based research showed that the visual perception of blue colour intensity is less distinct than the red and green colours. Secret message bits are embedded up to four bits of LSB, which are selected by a random number generator. The proposed algorithm was assessed on a set of RGB colour images, and satisfactory results were demonstrated regarding minimum distortion in the blue colour of a pixel and visually identical original and stego image.

Modern warehouse-scale computing facilities are based on thousands of independent computing nodes administered according to efficiency criteria that depend on workload. Networks play a pivotal role in these systems, as they are likely to be the performance bottleneck, and because of the high variability of data and management traffic. Because of the scale of the system, the prevalent network management model is based on autonomic networking, which requires routers capable of adapting their policies to traffic by a local or global strategy. In the article, 'Modelling performances of an autonomic router running under attack', co-authored by Campanile et al., the authors focus on performance modelling of autonomic routers, to provide a simple, yet representative elementary performance model which represents a starting point for a comprehensive autonomic network modelling approach. The proposed model is used to evaluate the behaviour of a router under attack under the realistic workload and parameter assumptions.

Editing this special issue has been a very demanding and stimulating experience since we dealt with several excellent contributions. To this aim, we would like to thank all the authors for their outstanding researches warmly. Each of the accepted articles has been subject to a rigorous peer-review procedure and has been assessed by several independent reviewers. Moreover, special thanks go to the anonymous reviewers, who provided constructive feedback to the authors to improve their works. Last but not least, we are grateful to the Editorial Board of this special issue and Prof. Kuan-Ching Li, Editor-in-Chief of the *International Journal of Embedded Systems*, for his great support throughout the entire publication processes.