Guest Editorial
Special Issue on Security and Forensics of Internet of Things: Problems and Solutions

THE Internet of Things (IoT) has experienced a significant growth over the last years and Gartner predicts that, by 2020, 21 billion IoT endpoints will be in use. The potential behind widespread usage of small devices capable of collecting, transmitting or acting upon data has been fueling the interest both from the industry and the academia. Security and forensics are two of the topics facing major challenges in this paradigm, on par with or even more prominent than other computing paradigms. Aspects such as low processing power and small storage capacity of such IoT devices contribute to their typically poor built-in security and forensics capabilities. Their reliance on Cloud Computing and mobile apps to operate and provide services increase the attack surface, distributing the collection of digital evidence and making reconstruction activities (to answer questions as what, where, when, who, why and how) harder.

Towards this end, this Special Issue approaches advancements in security and forensics solutions for the challenges that IoT systems have created. The Call for Papers was issued in April 2018, with the submission deadline set as 15 August 2018. We have received 56 submissions, from which 12 high-quality papers were selected.

The paper "LoRa-Key: Secure Key Generation System for LoRa-based Network", by Xu *et al.*, presented a protocol for generating keys on a Long Range (LoRa) network, through the usage of randomness in the Received Signal Strength Indicator (RSSI). The authors investigated the feasibility of key generation in indoor and outdoor environments, in both static and mobile scenarios, in terms of data rate and distance. They then developed the two main steps of the key generation protocol: signal processing, where data from the RSSI is filtered and then interpolated, and key generation, where the RSSI samples are converted into bits, and then passed through two other stages, reconciliation, to correct any potential errors, and privacy amplification, to avoid revealing too much information on the exchanged key. The authors performed a security analysis on their method, to evaluate the quality of the developed solution, and a performance analysis on entropy, bit rate, reconciliation method, and comparison to the IEEE 802.15.4 standard. Their results show that their method can correctly generate a key in two nodes under different environments, but low datarates is a problem left open for future work.

The paper "Enhancement of a Lightweight Attribute-Based Encryption Scheme for the Internet of Things", by Tan *et al.*, presented improvements to a lightweight key-policy attribute-based encryption (KP-ABE) scheme for the IoT. The authors argued that the original KP-ABE is not secure under Chosen-Plaintext Attack (CPA) due to the key generation algorithm being partially deterministic. They presented their solution and improvement of the encryption scheme, and extended it to support role delegation by means of a hierarchical KP-ABE (H-KP-ABE), mainly for application in decentralized systems. The performed tests show that the changes to the scheme have no impact on its performance, and the H-KP-ABE variant is compared to several other schemes, with the proposed scheme being among the fastest in terms of performance. While not being proven secure under a stringent model, the authors consider it to depict a good compromise between security and performance.

The paper "IoT Forensics: Amazon Echo as a Use Case", by Li *et al.*, presented a forensic model for IoT systems, capable of aiding in identification, preservation, analysis and presentation of forensic artifacts from IoT systems. The four stages work as follows. Identification first classifies the scenario, with IoT being a target, a tool or a witness for the alleged offense, and then attempts to identify all potential data sources, relevant time-periods, accessibility and data types. Preservation focuses on data extraction from the memory of the IoT device, be it volatile memory, storage, cache or other intermediate buffers. Analysis then delves into the data collected in the previous stage, that is then processed and finally compiled for the presentation stage. A practical use case is then elaborated by the authors for an Amazon Alexa enabled device, the Amazon Echo, using the proposed forensic model. The authors finally discussed several challenges for IoT forensics, such as the identification of data sources, the spread of evidence across different platforms (*e.g.*, cloud platforms that IoT systems can interact or integrate with), and the need to design forensics-friendly devices, to ease the collection of data.

The paper "Fractional-Order Spatial Steganography and Blind Steganalysis for Printed Matter: Anti-Counterfeiting for Product External Packing in Internet-of-Things", by Pu *et al.*, presented a construction for a Fractional-order Spatial Steganography (FSS) and a Fractional-order Blind Steganalysis (FBS) for printed materials. These apply to the IoT for anti-counterfeiting and tampering detection on, *e.g.*, packages, paper documents, currencies, paintings, or signatures, where it can be applied during transfer phases through the usage of IoT devices. According to the authors, digital steganography is traditionally not applicable to printed material. Their method

is capable of hiding information with FSS and detecting it through FBS, with their approach being resistant to statistics, rotation and distortion, cropping, scaling, noise, and colour copy attacks. The main challenges left open by the authors pertain to the improvement of the performance of the algorithms and benchmarking on mobile devices, and potential application of the methods to three-dimensional printable objects.

The paper "RSMA: Reputation System-based Lightweight Message Authentication Framework and Protocol for 5G-enabled Vehicular Networks", by Cui *et al.*, presented a protocol for authenticating messages in a 5G vehicular network, based on reputation, where a Trusted Authority (TA) defines the reputation of each vehicle, which will then be used as a threshold through which that vehicle is allowed or not to communicate with the network. The reputation system uses feedback given on the usefulness of messages sent by a given vehicle from other vehicles, that is then communicated to the TA, which filters and updates reputation locally, and then broadcasts to the network. The TA is also responsible for registering new vehicles, and providing credit reference (CR) and private key when the vehicle is considered trustworthy, so it can be part of the communication. The authors performed a security analysis on their framework and protocol, and analyzed the performance and computational costs in comparison to other schemes, concluding that the proposal had a lower communication cost. They also performed a working simulation of their system to demonstrate the validity of the reputation system.

The paper "Secure Beamforming Design in Relay-Assisted Internet of Things", by Huang *et al.*, presented a Cooperative Non-Orthogonal Multiple Access (NOMA) transmission scheme, where an IoT device harvests energy to aid another device to transmit. These schemes attempt to maximize the Secrecy Sum Rate (SSR) under three main constraints, transmission power, successive interference cancellation and quality of service, for which a Cooperative Simultaneous Wireless Information and Power Transfer (SWIPT) secure transmission protocol, an Artifical Noise (AN)-aided secure beamforming scheme for passive eavesdropping scenarios, and an orthogonal projection-based secure beamforming design scheme for active eavesdropping scenarios were developed and tested. The simulation results presented by the authors indicate a superior SSR performance when compared to other previously proposed schemes.

The paper "System Statistics Learning-Based IoT Security: Feasibility and Suitability", by Shinde *et al.*, presented a framework that uses system statistics to define the functioning of an IoT device and detect anomalies and problems through machine learning models. The authors tested three different predictive models for statistical learning to model the behaviour of an IoT system (linear regression, neural networks and recurrent neural networks) and compared their computation costs. In the anomaly detection phase, three statistical methods were used: local outlier factor, cumulative statistics threshold, and adaptive online thresholding. The models were trained and tested for each phase, with four different cyber attacks (unauthorized access, port scanning, flooding and virus infection), used to perform attack simulations and evaluate the performance of the different models and their effectiveness. It was concluded that linear regression and adaptive online thresholding exhibit the best compromise between performance and detection rate.

The paper "Chained Compressed Sensing: A Block-Chain-Inspired Approach for Low-cost Security in IoT Sensing", by Mangia *et al.*, proposed a solution for Compressed Sensing (CS) acquisition based on the blockchain technology, to enable secure data transmission between IoT nodes and a gateway. This CS, which acquires and compresses a signal that is then transformed into information (described as an analog-to-information interface) is used as a cryptographic primitive. In adapting the CS into a blockchain process, the CS behaves similarly to a block cipher. This is done over two variants, chaining measurements and sparse inputs. The authors then perform a security analysis, and show how their solution has some resistance, though not to the extent of the Advanced Encryption Standard (AES) (a compromise is made for better performance) to Known-Plaintext Attacks (KPA), Ciphertext-Only Attacks (COA), and Man-in-the-Middle (MitM) attacks when CS is used in the sparse inputs variant. They demonstrate that their solution provides a significant reduction in overhead when compared to AES in a practical example with a system for acquiring ECG data.

The paper "Groundwork for Neural Network-Based Specific Emitter Identification Authentication for IoT", by McGinthy *et al.*, presented a study on the usage of Neural Network (NN)-based Specific Emitter Identification (SEI) algorithms for authenticating IoT nodes on a network. The approach uses only In-phase and Quadrature (IQ) streams of the emitted signal to perform the authentication. A generic IoT model is defined, to try and adapt the algorithms. Three network topologies (star-of-stars, sparsely-connected mesh and densely-connected mesh) are defined, and devices are classified as edge devices, access points, central controllers and others. Three different approaches are explored: one-way SEI, mutual authentication through a secondary device, and authentication-as-a-service. Testing is then performed on two distinct devices, a Xeon server and Raspberry Pi Zero, to gauge performance on a central controller and edge device. The results show that, while feasible, improvements in latency and memory requirements are still needed, as well as improving the algorithms to be able to deploy them in more resource-constrained devices.

The paper "Physical Layer Security Enhancement for Internet of Things in the Presence of Co-channel Interference and Multiple Eavesdroppers", by Ssettumba *et al.*, presented a study on the impact of co-channel interference and the existence of eavesdroppers in the hybrid TAS/tSD physical layer security (PHY) scheme, which combines Transmit Antenna Selection (TAS) with threshold-based Switched Diversity (tSD). Two eavesdropping cases are approached: colluding and non-colluding. The authors also propose a power allocation model to improve secrecy performance through minimization of the Asymptotic Secrecy Outage Probability (ASOP). The tests conducted by the authors indicate that the proposed model has superior secrecy performance.

The paper "DER-TEE: Secure Distributed Energy Resource Operations through Trusted Execution Environments", by Se-

bastian *et al.*, presented a Trusted Execution Environment (TEE)-based architecture for smart inverters, capable of preventing tampering of telemetry data in smart power inverters (device that changes direct current into alternating current). The architecture is composed of three main components, a TEE, a Rich Execution Environment (REE), and a set of software tools that allow the REE to obtain data from applications running in the TEE. The architecture allows for secure auditing of the power output, protecting the system from having its telemetry data tampered with. To evaluate the system, an attack surface was defined, split between the attack surface of the TEE, the REE, and the communication between them. The obtained results showed that the architecture provides a secure way to audit the power output.

The paper "Detection and Isolation of False Data Inject Attack in Smart Grids via Nonlinear Interval Observer", by Wang *et al.*, presented a method for detection of false data inject attacks in smart grids. It is based on a nonlinear interval observer. The authors divided the grid into smaller grid subareas. To detect an attack on each subarea, the nonlinear interval observer takes into account external disturbances in a nonlinear dynamic model together with the measurement of the output of sensors in that subarea. The authors performed simulations of the false data inject attacks, and the achieved results showed the efficacy of the proposed detection and isolation algorithms.

Virginia N. L. Franqueira, *Guest Editor*
Department of Electronics, Computing & Mathematics
University of Derby, United Kingdom

Pedro Incio, *Guest Editor*
Department of Computer Science
Universidade da Beira Interior, Portugal

Aleksandra Mileva, *Guest Editor*
Faculty of Computer Science
University of Goce Delcev, Republic of Macedonia

Mauro Conti, *Guest Editor*
Department of Mathematics
University of Padua, Italy

Ville Leppnen, *Guest Editor*
Department of Information Technology
University of Turku, Finland

Raul H. C. Lopes, *Guest Editor*
College of Engineering, Design & Physical Sciences
Brunel University London, United Kingdom
JISC & CMS/CERN, United Kingdom

Virginia N. L. Franqueira received a Ph.D. in Computer Science (focused on Security) from the University of Twente (Netherlands) in 2009, and an M.Sc. in Computer Science (focused on Optimization) from the Federal University of Espirito Santo (Brazil). Since June 2014, she holds a senior lecturer position in Computer Security and Digital Forensics at the University of Derby, UK. She has around 40 publications related to Security or Digital Forensics. She is a member of the British Computer Society and fellow of The Higher Education Academy.

Pedro Ricardo Morais Incio holds a 5-year B.Sc. degree in Mathematics/Computer Science and a Ph.D. degree in Computer Science and Engineering, obtained from the Universidade da Beira Interior (UBI), Portugal, in 2005 and 2009 respectively. The Ph.D. work was performed in the enterprise environment of Nokia Siemens Networks Portugal S.A., through a Ph.D. grant from the Portuguese Foundation for Science and Technology.

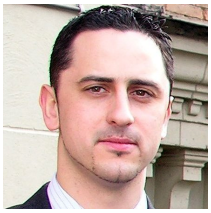
He is a professor of Computer Science at UBI since 2010, where he lectures subjects related with information assurance and security, programming of mobile devices and computer based simulation, to graduate and undergraduate courses, namely to the B.Sc., M.Sc. and Ph.D. programmes in Computer Science and Engineering. He is currently the Head of the Department of Computer Science of UBI. He is an instructor of the UBI Cisco Academy.

He is an IEEE senior member and a researcher of the Instituto de Telecomunicaes (IT). His main research topics are information assurance and security, computer based simulation, and network traffic monitoring, analysis and classification. He has about 30 publications in the form of book chapters and papers in international peer-reviewed books, conferences and journals. He frequently reviews papers for IEEE, Springer, Wiley and Elsevier journals. He has been member of the Technical Program Committee of international conferences such as the ACM Symposium on Applied Computing - Track on Networking.

Aleksandra Mileva was born in tip, Macedonia, in 1975. She obtained her Ph.D. degree in Computer Science from the Faculty of Natural Sciences and Mathematics Skopje, Ss. Cyril and Methodius University in Skopje in 2010.

She is an associate professor and a Vice dean at the Faculty of Computer Science, University Goce Delev in tip, Republic of Macedonia and Head of the Laboratory of Computer Security and Computer Forensics. From December 2018, she is a member of the EURASIP SAT on Biometrics, Data Forensics, and Security. She was a Management Committee member of two COST actions IC1201: BETTY and IC1306: Cryptography for Secure Digital Interaction. She is a coauthor and developer of the NaSHA family of hash functions, which was the First Round Candidate of the NIST SHA-3 Competition (2007-2012).

Her research interests include: digital steganography, cryptography, computer and network security, IoT protocols and security, and quasigroups theory.



Mauro Conti received his MSc and his Ph.D. in Computer Science (advisor Prof. Luigi V. Mancini) from Sapienza University of Rome, Italy, in 2005 and 2009, respectively. In 2008, he was Visiting Researcher (supervised by Prof. Sushil Jajodia) at the Center for Secure Information Systems (CSIS) at George Mason University, Fairfax, VA, USA . In 2009 he was selected for the ERCIM (European Research Consortium for Informatics and Mathematics) "Alain Bensoussan" Fellowship (currently a EU Marie Curie COFUND action). From 2009 to 2011 he was Postdoctoral Researcher (supervised by Prof. Andrew S. Tanenbaum and Prof. Bruno Crispo) at Vrije Universiteit Amsterdam, The Netherlands. In November 2010, he was visiting researcher at UCLA – University of California, Los Angeles, CA, USA (working with Prof. Mario Gerla). In 2011, he joined University of Padua, Italy , (among the best italian universities) as Assistant Professor (tenured faculty). In the summer of 2012, 2013, and 2014 he was visiting Assistant Professor at UCI – University of California, Irvine, CA, USA (working with Prof. Gene Tsudik). From 2012, he is a EU Marie Curie Fellow. In October-November 2013 he was a DAAD Fellow at the Center for Advance Security Research Darmstadt (CASED), TU Darmstadt, Germany (working with Prof. Ahmad-Reza Sadeghi). In 2014, he was elevated to the IEEE Senior Member grade. In 2015 he became Associate Professor, and Full Professor in 2018.

His research interests are mainly in the area of security and privacy. In this area, he published more than 170 papers in topmost international peer-reviewed journals and conferences, including IEEE TIFS, IEEE TDSC, IEEE TPDS, ACM TWEB, ACM/IEEE TON, IEEE TSC, IEEE COMST, ACM CCS, Usenix Security, ACM AsiaCCS, ACM WiSec, ACM SACMAT, ACM MobiHoc, ACNS, IEEE ICDCS, and ESORICS. He is Associate Editor for IEEE Communications Surveys & Tutorials and IEEE Transactions on Information Forensics and Security, and he served as Program Committee member of several conferences, including ACM AsiaCCS, ACM WiSec, ACM CODASPY, ACM SACMAT, IEEE INFOCOM, IEEE CNS, IEEE PASSAT, IEEE MASS, and ACNS. He was panelist at ACM CODASPY 2011, and panel chair at ICISS'16. He was General Chair for SecureComm 2012 and ACM SACMAT 2013, and Program Chair for TRUST 2015, ICISS'16, and WiSec'17.

Ville Leppnen is a full professor in software engineering and software security (since 2012) at the University of Turku, Finland. He received his PhD in 1996 (Computer Science) and has now over 220 international conference and journal publications. His research interests are related broadly to software engineering and security, ranging from software engineering methodologies, practices, and tools to security and quality issues, and to programming languages, parallelism, and architectural design topics. His security related research has focused on IoT and cloud security, software based diversification, vulnerability analyses, machine learning based profiling for host intrusion detection systems, introspection mechanisms, and fake service generation. Currently Leppnen serves as vice head of department and leader of 6 research and development projects.

Raul H. C. Lopes received a PhD in Computer Science from the School of Computer Studies at the University of Leeds in 1998, in the area of Computational Logic. He is an active member of the WLCG (Worldwide LHC Computing Grid) and CMS collaboration at Brunel University London and CERN Institute. He also works for Jisc/UK. His publications and work for WLCG, CMS and Jisc are concerned with all aspects of Grid and High Performance Computing, in particular, with algorithms and deployment of data analysis, new computer protocols, data transfer and storage technologies, and associated computer security and performance impact.