Digital Object Identifier 10.1109/ACCESS.2021.3101889

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: INTERNET-OF-THINGS ATTACKS AND DEFENSES: RECENT ADVANCES AND CHALLENGES

Internet of Things (IoT) technology has been widely adopted by the vast majority of businesses and is influencing every aspect of the world. However, the nature of the internet, communication means, embedded OS, and backend recourses make IoT objects vulnerable to cyber-attacks. For example, the Mirai botnet attack used the IoT to perform the DDoS attack that took down many popular websites. In addition, most standard and conventional security solutions designed for enterprise systems are not applicable to IoT devices. As a result, we are facing a big IoT security and protection challenge, and there is an urgent need to analyze current IoT-specific cyber-attacks and to design suitable and efficient security mechanisms.

The objective of this Special Section is to compile recent development and efforts dedicated to researching IoT attacks and defenses. The main purpose of this Special Section is to provide both academic and industry researchers a channel to discuss either practical or theoretical solutions to identify IoT vulnerabilities and relevant security mechanisms.

Due to the popularity of the IoT, we received a total of 99 submissions, of which 27 were accepted for publication. The selection is based on their novelty, contributions, and relevance. All articles underwent a thorough review process by at least two independent reviewers. The accepted articles are summarized below.

In the article titled ''Lightweight authentication protocol for NFC based anti-counterfeiting system in IoT infrastructure,'' Alzahrani *et al.* describe an authentication protocol for anti-counterfeited drug systems based on IoT, aiming to examine the validity of drug ''unit dosage.'' It uses near-field communication (NFC) and provides a security analysis under the random oracle model. After every successful transaction or process of verification, the NFC tag record can be updated in the repository. The evaluation was done by using Py-Charm tool.

In the article titled ''A top-k query scheme with privacy preservation for intelligent vehicle network in mobile IoT,'' by Zhou *et al.*, the authors devise a query scheme with vehicle privacy guarantees based on oblivious transfer (OT) and private information retrieval (PIR) in vehicle networks. They further achieve a more complicated Top-K query scheme, in which the neighbor vehicles cooperate with each other to transmit their encoded query interests, and service providers cannot decode the interest privacy for ranking popularity until enough data blocks are collected

The article by Chen *et al.*, ''Exploring Shodan From the perspective of industrial control systems,'' develops a distributed Industrial control systems (ICS) honeypot system that can capture attack data and recognize a large amount of Shodan scan traffic from the attack data. They then propose a hierarchical DFA-SVM traffic recognition model based on the function code and traffic features, which can improve the ability to identify Shodan and Shodan-like scans in honeypot data. They finally detect 29 Shodan scanners and 16 Shodan-like scanners verified by threat intelligence.

The article by Nasralla *et al.*, ''Defenses against perception-layer attacks on IoT smart furniture for impaired people,'' introduces an approach for providing defenses against perception-layer attacks on IoT smart pieces of furniture. Their approach uses DTW similarity for comparing input time series from specific sensor inputs in order to identify anomalies with a detector, which was previously trained from real normal data and some realistic potential perception-layer attacks. The benefit of applying time-series analysis is its capacity in detecting patterns considering the values as a part of a continuous series ordered in time and being able to usually detect more anomalies in certain IoT pieces of smart furniture.

The article by Lee *et al.*, ''On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks,'' presents an authentication protocol based on three-factors for WSNs and adopts the fuzzy-extractor for biometric awareness. The authors then show an authentication protocol by using the honey_list technique to defend against malicious attacks including stolen smartcards, identity guessing, password guessing, and replay attacks that can compromise the mutual authentication.

In the article ''A covert digital communication system using skewed α-Stable distributions for Internet of Things,'' by Xu *et al.*, the authors show how to encode the covert bit at the transmitter using the positive or negative transition of the skewness parameter of skewed α-stable distributions within the first and second halves of the one-bit period. A sample skewness estimator based on signed fractional lower order

moment (SFLOM) is used to determine the binary message at the receiver. Such scheme works in the physical layer with the advantages of simple structure and easy implementation with low-cost, resource-limited IoT devices exhibiting low-rate transmission.

The article by Hakak *et al.*, ''Have you been a victim of COVID-19-related cyber incidents? survey, taxonomy, and mitigation strategies,'' summarizes various COVID-19-related cyber threats, develops a new taxonomy of attacks and their effects on security goals, and discusses the potential mitigation strategies to counter the identified threats.

In the article ''Blockchain-based transaction validation protocol for a secure distributed IoT network,'' Hosen *et al.* introduce a blockchain-based transaction validation protocol for a secure distributed IoT network. It is a context-aware priority-based TX validation technique in a blockchain-enabled secure IoT network called CaBNet. The network adopts the SDN-gateway (GW), which acts as a bridge between the LLN and the blockchain network. SDN provides the network control and operations and executes different actions in counter to various vulnerabilities and attacks.

The article by Nasir *et al.*, ''Prioritization and alert fusion in distributed IoT sensors using Kademlia based distributed hash tables,'' presents a framework for alert reduction by introducing priority to each alert. The priority here is assigned by dynamically evaluating alerts and using several metrics such as severity, confidence, correlation, and service history. The Kademlia topology of DHT is used to prove that it is more efficient than previously used Chord. It can also offer load balancing among participating peers.

In the article by Le and Ngo, ''V-sandbox for dynamic analysis IoT botnet,'' the authors describe a set of dynamic features needed to detect IoT botnet using machine learning. Then, they present a new practical sandbox, named V-Sandbox, for dynamic analysis of the IoT botnet. This sandbox is an ideal environment for IoT botnet samples that exhibit malicious behavior. It can support the C&C server's connection, shared libraries for dynamic files, and a wide range of CPU architectures.

In the article ''Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey,'' by Sharma *et al.*, the authors describe the concept and ideology of smart M-IoT networks including their applications, advances, challenges, characteristics, technologies, and standards. Then, they emphasized approaches on secure frameworks, data-privacy, secure protocols, physical layer security, and handover protections for smart M-IoT. They discuss different ways for analyzing security, privacy, and trust in M-IoT followed by a roadmap and open issues.

In the article ''Privacy and security management in intelligent transportation system,'' Chavhan *et al.* introduce a privacy and security management scheme for supporting intelligent public transport system (IPTS) depots in metropolitan areas using an emergent intelligence (EI) technique. The proposed scheme is based on the integration of the transport depot staff policies, pseudonymous techniques, cryptographic techniques, bilinear pairing, and EI techniques. The proposed scheme provides accurate and reliable information to the transport depot agents, which can be shared with the neighbor depots' agents

The article by Wu *et al.* ''Research on artificial intelligence enhancing Internet of Things security: A survey,'' reviews the complexity of IoT security protection, and then identifies that Artificial Intelligence (AI) methods such as Machine Learning (ML) and Deep Learning (DL) can provide new powerful capabilities to meet the security requirements of IoT. The authors analyze the technical feasibility of AI in solving IoT security problems and summarize a general process of AI solutions for IoT security.

In the article ''Cybersecurity challenges associated with the Internet of Things in a post-quantum world,'' by Althobaiti and Dohler, the authors provide a comparative study of pre-quantum and post-quantum IoT security architectures and discuss how the 3G partnership project (3GPP) IoT security solutions fair in a post-quantum environment. They also analyze the security features of fifth-generation (5G) networks, and discuss the manner in which a quantum computer can compromise security.

In the article ''Trusted opportunistic routing based on node trust model,'' by Su *et al.*, the authors propose to use dynamic coefficients to balance direct trust and recommended trust, and introduce a trust model based on node behavior for detecting malicious nodes in the opportunistic routing and forwarding candidate set. The proposed trust model uses pruning and filtering mechanisms to remove malicious suggestions, and uses dynamic weight calculation methods to combine direct trust and indirect trust when calculating the comprehensive trust value, which can screen and filter low-trust nodes in the network.

In the article ''Secure data de-duplication based on threshold blind signature and bloom filter in Internet of Things,'' by Mi *et al.*, the authors focus on refraining redundancy and show a conspiracy-free data de-duplication protocol based on a threshold blind signature. With multiple key servers, the outsourced file and the de-duplication label could become computationally indistinguishable from random strings. They used the Boom filter as a tool to implement a proof of ownership, ensuring that the ownership claims made by users are real. It effectively prevents the attacker from using the stolen tag to get the whole file to gain file access without authorization.

In the article ''Multi-loss Siamese neural network with batch normalization layer for malware detection,'' by Zhu *et al.*, the authors introduce a strategy to convert a binary file, such as Andro-Dumpsys dataset, into image files that can feed into an N-shot based neural network model such as a Siamese Network. The proposed model is tuned such as way that it can work well on a small amount of training datasets. The multiple loss function is useful to improve the feature embedding space in the Siamese Neural Network for binary classification. In the feature embedding space, the distance of

each positive pair that belongs to the same class may become small.

In the article, ''Efficient BiSRU combined with feature dimensionality reduction for abnormal traffic detection,'' by Ding *et al.*, the authors design a way to apply the excellent feature learning capabilities of deep learning to achieve highly accurate network abnormal traffic detection. They first show a stack Sparse Auto-encoder (sSAE) to perform feature dimensionality reduction on the input traffic data. The sSAE can reduce the calculation amount and running time of the model. Then, they introduce a BiSRU based on Simple Recurrent Unit (SRU) to achieve parallel computing and accurate feature learning for abnormal traffic detection.

In the article ''Identification of critical nodes for enhanced network defense in MANET-IoT networks,'' by Niu *et al.*, the authors propose a dynamic critical node identification (DCNI) method to realize the identification of critical nodes in MANET-IoT networks through the application of port hopping mechanism on the identified critical nodes. They particularly show a comprehensive metric to measure the node importance in the topology snapshot. Afterwards, they introduce a sliding time window to filter out the topology snapshots, which have a close correlation with the current snapshot, and fuse the importance values of the same node in different topology snapshots. Then, the critical nodes are selected based on the ranking of fused importance.

The article by Ullah *et al.*, ''A lightweight and secured certificate-based proxy signcryption (CB-PS) scheme for E-prescription systems,'' presents a lightweight and provable secured certificate-based proxy signcryption scheme (CB-PS) for an E-prescription system. More specifically, they first explain the syntax of certificate-based proxy signcryption, and then present the construction certificate-based proxy signcryption (CB-PS) algorithm using the concept of the hyper elliptic curve. Also, they provide the network model for E-prescription system under the provided certificate-based proxy signcryption (CB-PS) scheme.

In the article ''SGF-MD: Behavior rule specification-based distributed misbehavior detection of embedded IoT devices in a closed-loop smart greenhouse farming system,'' by Astillo *et al.*, the authors show a lightweight specification-based distributed detection to identify the misbehavior of heterogeneous embedded IoT nodes in a closed-loop smart greenhouse farming system. To expand the monitoring space of a node, they exploited the Kalman-filter algorithm and simple statistical operations to obtain estimates of data. They express the behavior-rules as state machine diagrams based on the Unified Modeling Language (UML).

The article by An *et al.*, ''Securely outsource modular exponentiations with single untrusted cloud server,'' introduces two secure outsourcing schemes for fixed-base (public base and private exponent) and fixed-exponent (private base and public exponent) modular exponentiation. The schemes require only one untrusted server, and they later propose an efficient and secure Paillier encryption outsourcing scheme.

In the article ''Specific emitter identification against unreliable features interference based on time-series classification network structure,'' by Liu *et al.*, the authors focus on time-series classification method and propose a hybrid model, which is composed of the one-dimensional residual convolution network with dilated convolution and squeeze-and-excitation block (Conv-OrdsNet). They also apply a DBi-LSTM to solve the RF fingerprinting problem. They leverage a data augmentation method to alleviate the interference of power variation, frequency offset (FO), phase offset (PO), and channel noises.

In the article ''Privacy and security issues in deep learning: A survey,'' by Liu *et al.*, the authors introduce a total of four types of attacks and privacy-preserving techniques in deep learning (DL), including model extraction attacks, model inversion attacks, adversarial attacks, and poisoning attacks. They then review and summarize the attack and defense methods associated with DL privacy and security. To demonstrate the security threats in practice, they reviewed the adversarial attacks under the physical condition. They finally discuss current challenges and open problems regarding privacy and security issues.

In the article ''Cyber resilience in healthcare digital twin on lung cancer,'' by Zhang *et al.*, the authors show that vulnerability detection is a fundamental technology for cyber resilience in healthcare digital twins. They present a scheme for recognizing potential vulnerable functions to support healthcare digital twins. Also, they develop a deep neural model to capture bi-directional context relationships among the risky code keywords.

In the article ''Contextual trust model with a humanoid robot defense for attacks to smart eco-systems,'' by Abate *et al.*, the authors present the development and validation of a semantic trust model, which aggregates different ontologies for representing contextual information in relation to the environment and the users. Automatic reasoning is applied to user commands for evaluating the trust requirements. The requirements are then compared with the multi-biometry analysis performed by several smart devices and by an empowered version of the humanoid robot Pepper. The robot itself, including its interaction with the environment and every weakness exposed by the smart objects involved in its eco-system, may represent an exploit point for attacking the smart home and threaten IoT security and privacy.

In the article ''A study on the digital forensic investigation method of clever malware in IoT devices,'' by Kim *et al.*, the authors introduce some new types of files needed for investigating malware. First, they study how to analyze when and how malware penetrated devices by reversing the characteristics of social engineering techniques that can be used by malware. They study how to analyze the traces and timing of the installation of malware after infiltrating the device. They identified that the malware that first penetrated the device often being installed simply as a dropper and takes steps for the actual performance of malicious behavior. They then suggest how malware analyzes information from C&C

servers that leak information from stolen users and collect the information needed to trace back the hackers or groups of hackers that created the malware.

In conclusion, we would like to thank all the authors who submitted their research articles to our Special Section. We highly appreciate the contributions of the reviewers for their constructive comments and suggestions. We also would like to acknowledge the guidance and great support from the IEEE ACCESS Editor-in-Chief and staff members.

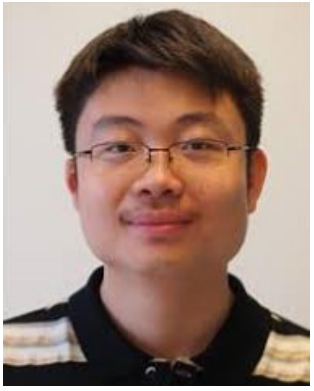
WEIZHI MENG, *Lead Editor*
Department of Applied Mathematics and Computer Science
Technical University of Denmark
2800 Kongens Lyngby, Denmark

JAVIER LOPEZ, *Guest Editor*
Department of Computer Science
University of Malaga
29016 Málaga, Spain

SHOUHUAI XU, *Guest Editor*
Department of Computer Science
University of Colorado at Colorado Springs
Colorado Springs, CO 80918, USA

CHUNHUA SU, *Guest Editor*
Division of Computer Science
The University of Aizu
Aizuwakamatsu 965-8580, Japan

RONGXING LU, *Guest Editor*
Faculty of Computer Science
University of New Brunswick
Fredericton, NB E3B 5A3, Canada



WEIZHI MENG (Senior Member, IEEE) received the Ph.D. degree in computer science from City University of Hong Kong (CityU), Hong Kong, in 2013. He is currently an Associate Professor with the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark. Prior to joining DTU, he worked as a Research Scientist with the Institute for Infocomm Research, A*Star, Singapore. His research interests include cybersecurity and intelligent technology in security, including intrusion detection, smartphone security, biometric authentication, HCI security, the IoT/CPS security, and blockchain in security. He won the Outstanding Academic Performance Award during his doctoral study. He was a recipient of the Hong Kong Institution of Engineers (HKIE) Outstanding Paper Award for Young Engineers/Researchers in 2014 and 2017. He has served as a program committee member for more than 50 international conferences. He was the PC Chair of IEEE Blockchain 2018, IEEE ATC 2019, IFIPTM 2019, and Socialsec 2019. He has also served as a Guest Editor for IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS (TII), *Future Generation Computer Systems* (FGCS), *Journal of Information Security and Applications* (JISA), *Sensors*, *Computer Applications in Engineering Education* (CAEE), *International Journal of Distributed Sensor Networks* (IJDSN), *Security and Communication Networks* (SCN), *Digital Communications and Networks* (DCN), and *Wireless Communications and Mobile Computing* (WCMC).

JAVIER LOPEZ (Senior Member, IEEE) is currently a Full Professor with the Computer Science Department, University of Malaga. His research interests include network security, security protocols, and critical information infrastructures, and leading a number of national and EU research projects in those areas. He is also a member of the Editorial Boards of *Wireless Communications*, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, *Computers & Security*, and *Journal of Computer Security*. In the past, he was the Chair of the IFIP Working Group 11.11 on Trust Management and the Chair of the ERCIM Working Group on Security and Trust Management. He is also the Co-Editor-in-Chief of *International Journal of Information Security* (IJIS).

SHOUHUAI XU (Senior Member, IEEE) received the Ph.D. degree in computer science from Fudan University. He is currently the Gallogly Chair Professor of cybersecurity with the Department of Computer Science, University of Colorado at Colorado Springs. He is also the Founding Director of the Laboratory for Cybersecurity Dynamics. He coined the notion of cybersecurity dynamics as a candidate foundation for the emerging science of cybersecurity. His research interests include the three pillar thrusts of cybersecurity dynamics: first-principle cybersecurity modeling and analysis, cybersecurity data analytics, and cybersecurity metrics. He co-initiated the International Conference on Science of Cyber Security and the ACM Scalable Trusted Computing Workshop. He is/was a Program Committee Co-Chair of SciSec2019, SciSec2018, ICICS2018, NSS2015, and Inscrypt2013. He is/was an Associate Editor of the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and the IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING.

CHUNHUA SU (Member, IEEE) received the B.S. degree from Beijing Electronic and Science Institute, in 2003, and the M.S. and Ph.D. degrees in computer science from the Faculty of Engineering, Kyushu University, in 2006 and 2009, respectively. He worked as a Research Scientist with the Cryptography and Security Department, Institute for Infocomm Research, Singapore, from 2011 to 2013. From 2013 to 2016, he worked as an Assistant Professor with the School of Information Science, Japan Advanced Institute of Science and Technology. From 2016 to 2017, he worked as an Assistant Professor with the Graduate School of Engineering, Osaka University. He is currently working as a Senior Associate Professor with the Division of Computer Science, The University of Aizu, Japan. His research interests include cryptanalysis, cryptographic protocols, privacy-preserving technologies in data mining, and IoT security and privacy.

RONGXING LU (Fellow, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2012. He has been an Assistant Professor with the Faculty of Computer Science, University of New Brunswick (UNB), Fredericton, NB, Canada, since August 2016. Before that, he worked as an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore, from May 2013 to August 2016. He worked as a Postdoctoral Fellow with the University of Waterloo, from May 2012 to April 2013. His research interests include applied cryptography, privacy enhancing technologies, and the IoT-big data security and privacy. He has published extensively in his areas of expertise. He was a recipient (with his students and colleagues) of the Student Best Paper Award, the ITS Summit Singapore 2015, the IEEE IES Student Best Paper Award 2014, the Best Paper Awards of *Tsinghua Science and Technology* Journal 2014, IEEE ICCC 2015, IEEE WCNC 2013, BodyNets 2010, and IEEE ICCCN 2009. He was awarded the most prestigious "Governor General Gold Medal," for his Ph.D. degree. He won the 8th IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award, in 2013. He was/is on the editorial boards of several international refereed journals, e.g., *IEEE Network*. He has served/serves as the Technical Symposium Co-Chair for IEEE GLOBECOM'16 and many technical program committees for IEEE and other international conferences, including IEEE INFOCOM and ICC. He also serves as the Secretary for the IEEE Communications and Information Security Technical Committee (ComSoc CIS-TC). He is also the Winner of the 2016–2017 Excellence in Teaching Award, FCS, and UNB.