Mobile Networks and Applications (2022) 27:343–345
https://doi.org/10.1007/s11036-021-01872-9

Editorial: Security and Privacy Challenges in Internet of Things

Ding Wang[1,2] · **Weizhi Meng**[3]

Accepted: 23 November 2021 / Published online: 8 December 2021

1 Contents

2 Editorial

The rapid advancements in mobile networks and applications have brought great changes to the existing computing paradigms and computing environments. Mobile computing, big data, and cyberspace-based supporting technologies such as Cloud Computing, Cyber-Physical Systems, Blockchain, and other large-scale computing environments are becoming an integral part of our daily life, and Internet-of-Things (IoT) is becoming more and more realistic. For example, being adopted in more and more fields, IoT is making "Everything Smart," such as smart home, smart manufacturing, smart city, and smart transportation, among which, there are many security-critical areas. Although researchers continue to tackle IoT security and privacy issues, many questions remain unsolved. For example, how access control and authentication in the new IoT computing environments should and will be? How to effectively apply new cryptographic techniques for new IoT computing environments? How to protect the security and privacy of entities in IoT? Further, with the growing adoption of IoT devices, there is a growth in the number of security and privacy issues. This special issue aims to answer the above questions to some extent and solicits extensions of best-quality papers from the 3rd EAI International Conference on Security and Privacy in New Computing Environments (EAI SPNCE 2020).

This special issue features nine selected papers with high quality. The first article, "A secure access control framework for cloud management", authored by Jiawei Zhang et al., proposed a secure access control framework suitable for resource-centric Cloud operating system in order to overcome privilege abuse caused by RBAC policy rules tampering or token hijack. For one thing, the authors proposed a new authorization model with cryptographically protected RBAC policy rules. For another thing, the authors achieved user token unlikability and token-replay-attack resistance

✉ Weizhi Meng
weme@dtu.dk

[1] College of Cyber Science, Nankai University, Tianjin 300350, China

[2] Tianjin Key Laboratory of Network and Data Security Technology, Nankai University, Tianjin 300350, China

[3] DTU Compute, Technical University of Denmark, Kgs. Lyngby 2800, Denmark

by introducing random element and leveraging one-show token technique.

The second article titled "An Adaptive IoT Network Security Situation Prediction Model" presented the motivation for effectively predict the network security situation of the IoT and proposed an adaptive IoT network security situation prediction model, which makes the accuracy of IoT network security situation prediction higher.

In the next article with the title "Towards Multi-user Searchable Encryption Scheme with Support for SQL Queries", the authors studied the searchable encryption problem to solve the data privacy disclosure caused by outsourcing data to cloud servers. The authors proposed a multi-user shared searchable encryption scheme that supports multi-user selective authorization and secure access to encrypted databases. Specifically, the authors apply the Diffie-Hellman protocol to a trapdoor generation algorithm to facilitate fine-grained search control without incremental conversions, then they utilized a private key to generate an encrypted index by bilinear mapping, which makes it impossible for an adversary to obtain trapdoor keywords by traversing the keyword space and to carry out keyword guessing attacks. Finally, the authors use double-layered encryption to secure a symmetric decryption key. Only the proxies whose attributes are matched with the access control list can obtain the key of decrypted data.

Fog computing is a new computing paradigm in the era of the Internet of Things. The fourth article titled "Support Vector Machine Intrusion Detection Scheme Based on Cloud-Fog Collaboration" proposed a lightweight support vector machine intrusion detection model based on Cloud-Fog Collaboration (CFC-SVM). Due to the high dimensionality of network data, first, Principal Component Analysis (PCA) is used to reduce the dimensionality of the data, eliminate the correlation between attributes and reduce the training time. Then, in the cloud server, a support vector machine (SVM) optimized by the particle swarm algorithm is used to complete the data training, obtain the optimal SVM intrusion-detection classifier, send it to the fog node, and carry out attack detection at the fog node.

Wearable electronic equipment and wireless communications provide convenience to the patients. Wireless body area network has benefited our lives by assisting in making medical diagnosis. The fifth article, "A Certificateless Authentication and Key Agreement Scheme for Secure Cloud-assisted Wireless Body Area Network" identified security risks in a cloud-assisted authentication protocol and designed a new anonymous certificateless authentication scheme. The scheme can ensure a secure and communication channel between the wearable devices and the cloud server.

With the development of 5G technology, Internet of Things (IoT) is proliferating and deeply integrated with our daily lives and industry productions. IoT applications in the 5G era generate massive connections, and this would bring about many security issues. The sixth article titled "Security Standards and Measures for Massive IoT in the 5G Era" analyzed the security risks for massive IoT in the 5G era. The authors summarized related security policies and standards. Furthermore, they identified security requirements and measures for various layers, including sensor control equipment and IoT card, IoT network and transmission exchange, IoT business application and service, and IoT security management and operation. Finally, in order to promote the secure development of IoT in the 5G era, the authors also provided some suggestions on IoT security technology and standardization work.

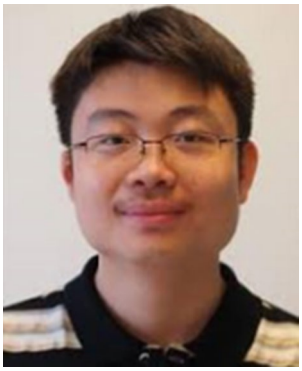
Data protection is becoming more and more important on smartphones, since people often store a lot of personal data like images on the device and use it for completing sensitive tasks such as online payment and financial transfer. The seventh article, "DCUS: Evaluating Double-Click-based Unlocking Scheme on Smartphones" proposed DCUS, a double-click based unlocking scheme on smartphones, which requires users to unlock the device by double clicking on the right location on an image. By checking the selected images, image location and double-click patterns, this scheme can achieve good user authentication.

The eighth article titled "Use of Behavior Dynamics to Improve Early Detection of At-risk Students in Online Courses" presented the motivation for quickly and accurately identify students at risk of failing their course during an online learning course and proposed a long-short term memory (LSTM) network-based approach to identify at-risk students.

Network Intrusion Detection Systems (NIDSs) are an important tool for protecting computer networks against increasingly sophisticated cyber-attacks. The last article titled "Towards a Standard Feature Set for Network Intrusion Detection System Datasets" proposed and evaluated standard NIDS feature sets based on the NetFlow network meta-data collection protocol, which aims to solve the NIDS problem of lacking a standard feature set. The authors converted four widely used NIDS datasets (UNSW-NB15, BoT-IoT, ToN-IoT, CSE-CIC-IDS2018) into new variants with their proposed NetFlow based feature sets.

Acknowledgement The guest editors are thankful to our reviewers for their great effort in reviewing the manuscripts. We also thank the Edit-in-Chief, Dr. Imrich Chlamtac for his supportive guidance during the entire process. The launch of this special issue was in part supported by the National Natural Science Foundation of China under Grant No. 62172240.

Ding Wang received his Ph.D. degree in Information Security at Peking University in 2017, and was supported by the "Boya Postdoctoral Fellowship" in Peking University from 2017 to 2019. Currently, he is a Full Professor at Nankai University. As the first author (or corresponding author), he has published more than 60 papers at venues like IEEE S&P ACM CCS, NDSS, Usenix Security, IEEE TDSC, and IEEE TIFS. His research has been reported by over 200 medias like Daily Mail, Forbes, IEEE Spectrum and Communications of the ACM, appeared in the Elsevier 2017 "Article Selection Celebrating Computer Science Research in China", and resulted in the revision of the authentication guideline NIST SP800-63-2. He has been involved in the community as a TPC member/PC Chair for over 60 international conferences such as PETS 2022, ACSAC 2021/2020, ACM AsiaCCS 2022/2021, IFIP SEC 2018-2021, ICICS 2019-2022. He has received the "ACM China Outstanding Doctoral Dissertation Award", the Best Paper Award at INSCRYPT 2018, and the First Prize of Natural Science Award of Ministry of Education. His research interests focus on passwords, authentication, and provable security.



Weizhi Meng 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 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, IoT/CPS security, and blockchain security. He won the Outstanding Academic Performance Award during his doctoral study, and was a recipient of the Hong Kong Institution of Engineers (HKIE) Outstanding Paper Award for Young Engineers/Researchers in 2014 and 2017. He has also served as a Guest Editor for IEEE Transactions on Industrial Informatics, 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), etc.