Guest Editorial Special Section on Security, Privacy, and Trust for Consumer Smart Devices

CURRENTLY, smart devices such as smartphones have become common and essential in our daily lives, which provide many new intelligent services. For example, consumers will use their smart devices for online purchase and personal data storage. In the context of Internet-of-Things (IoT), smartphones and household appliances can be seen as sensor nodes and compose sensor networks for measuring environmental parameters and generating user interaction data. These connections also offer novel use cases and customized experiences that are attractive to both manufacturers and consumers. The consumer electronics market is predicted to reach at a Compound Annual Growth Rate (CAGR) of 5.2% from 2023–2033.

However, the security, privacy and trust of consumer smart devices are threatened by various cyber-attacks. For instance, it still remains a challenge to protect the stored data on the smart devices under malicious applications, and to securely transfer confidential data over IoT in the presence of eavesdroppers and other attackers that may intercept and disrupt the information exchange between legitimate terminals remains to be a challenging research task. There is a significant need to secure smart devices in the aspect of security, privacy and trust.

Based on the above challenges, this Special Section on Security, Privacy and Trust for Consumer Smart Devices focused on consumer smart devices, and aimed to solicit original research papers that discuss the security, privacy and trust issues and solutions.Overall, 17 submissions were received spanning different CE domains, which were reviewed by at least three experts in the fields. In the end, five papers were ultimately accepted.

In [A1], the authors introduced a collision penalty (CP)-based mechanism to counter attacks in different scenarios regarding Cognitive Radio (CR) technology. They first formalize the attack scenarios, and then introduce a suitable mathematical bounds. The authors compared their mechanism with several jammer schemes, figuring out that the proposed CP-based mechanism can reach up to 700% malicious utility reduction in the best case. Under the current Moral Hazard Principal Agent (MHPA) model, the authors could obtain an expression for the expected gain of the unlicensed smart devices.

In [A2], the authors presented a GAN-based encryption method to secure digital images. In particular, the authors first provided a pseudo-random number generator strategy based on GAN to generate a secure key for the encryption with logistics and Henon map. The encrypted images can be down-sampled into one-fourth of the original size. A customized super-resolution network (CSRNet) was finally proposed to reconstruct the original images from the down-sampled images. The evaluation was performed on the Kodak 24 and T91 datasets, and the results indicated that the difference between these two encrypted images is 99.71%. The results demonstrated that the proposed scheme can efficiently withstand brute force attacks and is highly sensitive to encryption keys.

In [A3], the authors identified that the security of Android unlock pattern is weak in practice, and proposed an enhanced Android unlock scheme based on Pinch-to-Zoom actions on smartphones, called ZoomPass. This scheme includes two general steps: first, a user has to choose one dot and perform a Pinch-to-Zoom action, and then the user has to select the second dot and perform another Pinch-to-Zoom action. In the first user study, the scheme investigated the performance of supervised learning algorithms with 40 participants, and the authors selected SVM classifier in the implementation. In the second user study with 60 participants, the authors compared the scheme performance between ZoomPass and Double Patterns and DeLuca scheme. The results indicated that the proposed ZoomPass could reach better performance than the other schemes in the aspects of security and usability.

In [A4], the authors introduced a revocable and lightweight access control (ReLAC) with blockchain for smart consumer electronics. In particular, their method can reach efficient storage and outsourced decryption, for example, ReLAC stores encrypted files and ABE ciphertexts on IPFS and blockchain respectively. The proposed method can also provide partial hiding of the access policy and secure deduplication. ReLAC leverages the message-locked encryption (MLE) and the underlying hash deduplication function of IPFS to provide efficient and secure deduplication. Furthermore, in the proposed scheme, ciphertext updating will not be affected by attribute numbers, providing both forward and backward security.

In [A5], the authors extended the previous work and proposed an efficient certificateless online/offline signcryption (CLOOSC) based on the certificateless public key cryptosystem. The proposed scheme does not need a certificate management, which can avoid associated complexities and potential key escrow issues. It is designed based on elliptic curve cryptography, which can avoid the usage of

Digital Object Identifier 10.1109/TCE.2023.3347456

expensive bilinear pairings and HashToPoint operations. It can also greatly improve the computational efficiency and reduce communication overhead. The signcryption completes the encryption and signature in a single step. The analysis demonstrated that the proposed scheme could reach obvious-performance advantages and was more suitable for smart home consumer electronics.

It has been a great privilege for us to be able to serve this special issue as guest editors. We would like to take this opportunity to thank Professor Kim Fung Tsang, the Editor-in-Chief of IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, for approving our initial proposal on having a special issue on this subject, and his constant support and encouragement.

APPENDIX: RELATED ARTICLES

[A1] S. Shrivastava, S. John, A. Rajesh, and P. K. Bora, "Collision penalty-based defense against collusion attacks in cognitive radio enabled smart devices," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3963–3976, Feb. 2024.

[A2] M. Singh, N. Baranwal, K. N. Singh, and A. K. Singh, "Using GAN-based encryption to secure digital images with reconstruction through customized super resolution network," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3977–3984, Feb. 2024.

[A3] W. Li, T. Gleerup, J. Tan, and Y. Wang, "A security enhanced android unlock scheme based on pinch-to-zoom for smart devices," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3985–3993, Feb. 2024.

[A4] J. Zong, C. Wang, J. Shen, C. Su, and W. Wang, "ReLAC: Revocable and lightweight access control with blockchain for smart consumer electronics," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3994–4004, Feb. 2024.

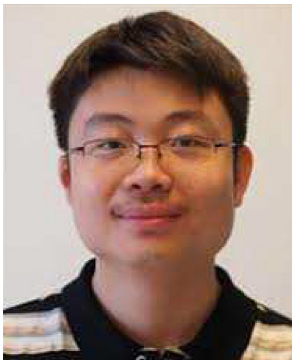
[A5] H. An, D. He, C. Peng, M. Luo, and L. Wang, "Efficient certificateless online/offline signcryption scheme without bilinear pairing for smart home consumer electronics," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 4005–4015, Feb. 2024.

WEIZHI MENG
DTU Compute
Technical University of Denmark
2800 Kongens Lyngby, Denmark

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

JUN ZHANG
Department of Computing Technologies
Swinburne University of Technology
Hawthorn, VIC 3122, Australia

PIERANGELA SAMARATI
Computer Science Department
Università degli Studi di Milano
20122 Milan, Italy



Weizhi Meng (Senior Member, IEEE) received the Ph.D. degree in computer science from the City University of Hong Kong, Hong Kong, SAR. 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, Singapore. He is currently directing the SPTAGE Lab, DTU Compute, DTU. His primary research interests are cyber security and artificial intelligent in security including intrusion detection, smartphone security, biometric authentication, trust management, and vulnerability analysis. He won the Outstanding Academic Performance Award during his doctoral study, and is a recipient of The HKIE Outstanding Paper Award for Young Engineers/Researchers in 2014 and 2017. He is an Editor for many reputed journals, such as IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE ACCESS, *Journal of Information Security and Applications*, *Journal of Ambient Intelligence and Humanized Computing*, and *International Journal of Information Security*.

Rongxing Lu (Fellow, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2012. He is a Mastercard IoT Research Chair, a University Research Scholar, an Associate Professor with the Faculty of Computer Science, University of New Brunswick, Canada. Before that, he worked as an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from April 2013 to August 2016. He worked as a Postdoctoral Fellow with the University of Waterloo from May 2012 to April 2013. He has published extensively in his areas of expertise (with citation 25 500+ and H-index 79 from Google Scholar as of March 2022). His research interests include applied cryptography, privacy enhancing technologies, and IoT-Big Data security and privacy. During his Ph.D., he was awarded the most prestigious "Governor General's Gold Medal." He won the 8th IEEE Communications Society Asia Pacific Outstanding Young Researcher Award in 2013. He was the recipient of nine best (student) paper awards from some reputable journals and conferences. He currently serves as the Chair of IEEE Communications and Information Security Technical Committee, and the founding Co-Chair of IEEE TEMS Blockchain and Distributed Ledgers Technologies Technical Committee. He is the Winner of 2016–17 Excellence in Teaching Award, FCS, and UNB. In the 2022 Edition of Research.com Ranking of Top 1000 Scientists in the field of Computer Science, he has been ranked 572 in the world ranking and 22 in Canada. For more information, see https://research.com/u/rongxing-lu.

Jun Zhang (Senior Member, IEEE) is a Full Professor and the Director of the Cybersecurity Lab, Swinburne University of Technology, Australia. He was recognized in the Australian's top researcher's special edition publication as the leading researcher in the field of computer security and cryptography in 2020. He works closely with distinguished colleagues. His cybersecurity lab conducts world-class research and fosters cross-disciplinary collaboration with solid support from ARC, CSIRO, DSTG, and many industry partners. The outputs include many high impact research papers and multi-million-dollar research projects, which significantly contributes to Swinburne's rankings in ARWU, QS, THE, and ERA. He created a cybersecurity teaching team with the Swinburne University of Technology, developed an industry-driven teaching model, and achieved a smooth online transition during the pandemic. He has been serving as a Steering Committee Member of the P-TECH Program at Melbourne since 2019, which the Australian Government invested in, promoting STEM education in secondary schools. He devotes himself to communication and community engagement, boosting the awareness of cybersecurity.

Pierangela Samarati (Fellow, IEEE) is a Professor with the Computer Science Department, Università degli Studi di Milano. She has been a Computer Scientist with the Computer Science Laboratory, SRI, CA, USA. She has been a Visiting Researcher with the Computer Science Department, Stanford University, CA, USA, and with the Center for Secure Information Systems, George Mason University, VA, USA. She is the Coordinator of the Working Group on Security of the Italian Association for Information Processing, the Italian representative in the International Federation for Information Processing Technical Committee 11 on "Security and Privacy." Her main research interests are in data protection, security, and privacy. She has received the ESORICS Oustdanding Research Award in 2018, the IEEE Computer Society Technical Achievement Award in 2016, the IFIP TC11 Kristian Beckman Award in 2008, and the IFIP WG 11.3 Outstanding Research Contributions Award in 2012. She has coordinated and participated in several projects, funded by the European Commission and the Italian Ministry or Research. She is a member of the Steering Committee of: European Symposium on Research in Computer Security, IEEE Conference on Communications and Network Security, Italian Conference on CyberSecurity, International Conference on Information Systems Security, and International Conference on Information and Communications Security. She is the Chair of the IEEE Systems Council Technical Committee on Security and Privacy in Complex Information Systems, the ERCIM Security and Trust Management Working Group, and the ACM Workshop on Privacy in the Electronic Society. She is an ACM Fellow in 2021, an IFIP Fellow in 2021, and an ACM Distinguished Scientist in 2009.