Editorial

User Authentication in the IoE Era: Attacks, Challenges, Evaluation, and New Designs

Ding Wang¹, Shujun Li², and Qi Jiang³

¹*School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China*

²*School of Computing, University of Kent, Canterbury CT2 7NF, UK*

³*School of Cyber Engineering, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Ding Wang; wangdingg@pku.edu.cn

Received 25 February 2018; Accepted 25 February 2018; Published 14 May 2018

Copyright © 2018 Ding Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We are venturing into the new era of Internet of Everything (IoE) where smaller and smarter computing devices have begun to be integrated into our environments. Despite its great potential, IoE also exposes devices to new security and privacy threats, such as the exposure of devices to attacks emanating from the Internet. User authentication, as a first line of defense, has been widely deployed to prevent unauthorized access, and, in many cases, it is also the primary line of defense.

However, conventional user authentication mechanisms are not capable of dealing with this new situation. Firstly, it is not possible to directly utilize Internet-centric security solutions because of the inherently heterogeneous characteristics of IoE devices (e.g., the limited computational capabilities and power supply). Secondly, constrained devices may lack conventional user interfaces, such as keyboard, mice, and touch screen. In summary, the subjects of authentication in IoE are compelling yet largely unexploited, as well as unexplored topics that are in need of more intense interest and research from both the industry and academia.

This special issue aims to provide a forum for researchers to publish and exchange their recent research ideas and results about authentication in IoE. In response to the call for papers, after rigorous review and careful revision, the following 5 papers were included in this special issue, ranging from novel understanding of traditional textual passwords, new cryptographic primitives for user authentication, and privacy-preserving biometric authentication to interesting contemporary key users authentication in microblogging.

The paper “An Alternative Method for Understanding User-Chosen Passwords” by Z. Zheng et al. sheds light on how to transform a dataset of passwords into a password graph by regarding passwords as vertices, introduces some novel notions from graph theory and report on a number of inner properties of passwords from the perspective of graph, and also visualizes five graphs of real-world password datasets to deliver an intuitive grasp of user-chosen passwords.

The paper “An Aggregate Signature Based Trust Routing for Data Gathering in Sensor Networks” by J. Tang et al. presents a new aggregate signature based trust routing scheme (named ASTR) to guarantee safe data collection in WSNs. The ASTR scheme adopts the aggregate signature approach and a trust routing method to improve the security of routing. The theoretical analysis results show that the ASTR scheme can effectively increase the safe reach rate of data routing by 23.23%, reduce the data amount on the node by 53.95%, and reduce the redundant data amount by 41.70%.

The paper “Comparable Encryption Scheme over Encrypted Cloud Data in Internet of Everything” by Q. Meng et al. points out that, in traditional cloud-based databases, short comparable encryption (SCE) schemes have been widely used by authorized users to conduct comparable queries over ciphertexts, but existing SCE schemes still incur high storage and computational overhead as well as economic burden. In this paper, the authors first propose a basic short comparable encryption scheme based on sliding window method, which can significantly reduce computational and storage burden as well as enhance work efficiency.

The paper “Privacy-Preserving Biometric Authentication: Challenges and Directions” by E. Pagnin and A. Mitrokotsa reviews and categorizes the most challenging issues that need to be taken into consideration when designing secure and privacy-preserving biometric authentication protocols. More precisely, the authors describe the main threats against privacy-preserving biometric authentication systems and give directions on possible countermeasures in order to design secure and privacy-preserving biometric authentication protocols.

The paper “Information Propagation Prediction Based on Key Users Authentication in Microblogging” by M. Yu et al. proposes a novel linear model based on key users authentication in microblogging. This model mines key users to dynamically improve the linear model while predicting information propagation. It can not only predict information propagation but also mine key users. Experimental results show that it can achieve remarkable efficiency in predicting information propagation.

Acknowledgments

We would like to thank all of the authors who have submitted their research to this special issue. We would also like to thank all the reviewers who have participated in the review process of the articles submitted to this special issue and provided helpful suggestions to the authors for improving their work. The launch of this special issue was in part supported by the National Key Research and Development Plan under Grant no. 2016YFB0800603. We hope that this special issue will advance the understanding and research of user authentication in the IoE era. We hope that the readers enjoy the papers.

*Ding Wang
Shujun Li
Qi Jiang*