Guest Editor's Introduction to the Special Section on Social Network Security

Meikang Qiu, *Senior Member, IEEE*, Yang Xiang, *Senior Member, IEEE*, and Yan Zhang, *Senior Member, IEEE*

THE emerging paradigm of social network provides an enormous number of novel approaches to implementing advanced networking communications and data analysis schemes efficiently using existing datasets, networks, and infrastructure. Social networks have had a great impact on people's daily life and global businesses, as has been addressed by recent research. However, the security issue is also a critical concern when adopting social network technologies in practice. Considering the uniqueness of social networks, the mechanism is now facing a variety of security challenges from multiple dimensions, such as mobile apps, wireless communication, cloud systems, big data, and security operations. Compared with traditional security issues, the applications of social networks are operated in a dynamic circumstance involving different internal and external inputs and factors, which requires new security mechanisms in distinct operational environments. The complexity of the technical implementations may result in unexpected consequences when adopting social network technologies. It is therefore important for current researchers and practitioners to address the security issues and seek out efficient ways to handle different hazards. For the purpose of preventing social network-based solutions from the threats of social networks, a variety of cyber security approaches or mechanism have been proposed. This special issue concentrates on the challenging topic–"Social Network Security" and aims to invite the cutting-edge academic achievements to be submitted here.

This special issue has collected 58 submissions and 9 of them were eventually accepted to appear in this issue. Each accepted article has been assessed by a careful review and evaluation process. The decisions considered both research quality and variety of topics. We organized the articles into four topics, which are advanced persistent threats in social network, privacy protection in social network, secure mobile social network architecture, and risk analysis and data governance in social network dimensions.

First, three articles on the advanced persistent threats in social networks were accepted. Part 1: Khan et al. introduced the rise in use of Online Social Networks (OSNs) which brings out insecure activities, such as the existence of spammers sending illegal emails and the polluted results of recommendation systems some legitimate users caused. They proposed a framework to segregate such type of users from real experts in particular field which adopts modified Hyperlink Induced Topic Search based on Twitter considering the domain specific keywords in the tweets and several other tweet characteristics. Part 2: Cresci et al. focused on the challenging problem of spambot detection in social network. They proposed a novel spambot detection method by leveraging digital DNA sequence, which is superior in spambot detection capability. Part 3: Cai et al. explored how to launch an interface attack exploiting social networks with a mixture of non-sensitive attributes and social relationships. This is the first work that employs collective methods involving various data-manipulating methods and social relationships to protect against inference attacks in social networks.

Next, on the topic of privacy protection in social networks we accepted two articles. Part 4: Wang et al. showed that a wide spread use of data mining applications had brought out a huge threat to mobile users' privacy due to the release of crowd-sources social network data to the public. They designed an online aggregate monitoring framework over infinite streams with w-event privacy guarantee-RescueDP to provide privacy-preserving statistics and an enhanced RescureDP with neural networks to predict the values of statistics and improve the utility of released data accurately. Part 5: Zhang et al. presented a novel human-to-human infection analysis approach by exploiting social network data and health data that are collected by social network and e-healthcare technologies.

Also, we accepted three articles in the dimension of secure mobile social network architecture. Part 6: Guerar et al. presented an overview of identity authentication mechanism in mobile social network. The proposed approach introduces screen brightness as a random input of PIN-based identity authentication, which can resist unauthorized access attacks in mobile social network. Part 7: He et al. proposed a new framework for the handshake scheme in MHSNs, which is based on hierarchical identity-based cryptography. The article then proved the security of the scheme, and a comparative summary demonstrates that the proposed scheme requires fewer computation and lower communication costs. Part 8:

- *M. Qiu is with the Columbia University, New York, NY 10027. E-mail: mq2203@columbia.edu.*
- *Y. Xiang is with the Swinburne University of Technology, Hawthorn, VIC 3122, Australia. E-mail: yxiang@swin.edu.au.*
- *Y. Zhang is with the University of Oslo, Oslo 0315, Norway. E-mail: yanzhang@ieee.org.*

For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TDSC.2018.2841441

Li et al. studied location privacy leakage from MSNs by matching the users' shared locations with their real mobility traces. The article also proposed SmartMask, a context-based system-level privacy protection solution, designed to automatically learn users' privacy preferences under different contexts and provide a transparent privacy control for MSN users.

Finally, one accepted article is on risk analysis and data governance in social networks. Part 9: Alrubaian et al. addressed the challenging task of information credibility assessment on Twitter. The proposed solution enabled to prevent rumor/fake information diffusion by assessing information credibility.

We hope that the achievements gathered in this special issue will be of timely value to readers of IEEE Transactions on Dependable and Secure Computing.

Meikang Qiu
Yang Xiang
Yan Zhang
Guest Editors

Meikang Qiu received the BE and ME degrees from Shanghai Jiao Tong University and the PhD degree in computer science from the University of Texas at Dallas. Currently, he is a faculty member with Columbia University. He is the chair of the IEEE Smart Computing Technical Committee. His research interests include cyber security, big data analysis, cloud computing, smarting computing, intelligent data, embedded systems, etc. A lot of novel results have been produced and most of them have already been reported to research community through high-quality journal and conference articles. He has published 4 books, 400 peer-reviewed journal and conference articles (including more than 200 journal articles, more than 200 conference articles, more than 70 IEEE/ACM Transactions articles). His paper published in the *IEEE Transactions on Computers* about privacy protection for smart phones has been selected as a Highly Cited Paper in 2017. His paper about embedded system security published in the *Journal of Computer and System Science* (Elsevier) have been recognized as Highly Cited Papers in both 2016 and 2017. His paper about data allocation for hybrid memory has been published in the *IEEE Transactions on Computers* has been selected as hot paper (1 in 1,000 articles) in 2017. His paper on Tele-health system has won the *IEEE System Journal* 2018 Best Paper Award. He also won the *ACM Transactions on Design Automation of Electrical Systems* (TODAES) 2011 Best Paper Award. He has won another more than 10 Conference Best Paper Awards in recent years. Currently, he is an associate editor of more than 10 international journals, including the *IEEE Transactions on Computers* and the *IEEE Transactions on Cloud Computing*. He has served as leading guest editor of the *IEEE Transactions on Dependable and Secure Computing* (TDSC), special issue on Social Network Security. He is the general chair/program chair of a dozen of IEEE/ACM international conferences, such as IEEE TrustCom, IEEE BigDataSecurity, IEEE CSCloud, and IEEE HPCC. He has won Navy Summer Faculty Award in 2012 and Air Force Summer Faculty Award in 2009. His research is supported by US government such as NSF, NSA, Air Force, Navy and companies such as GE, Nokia, TCL, and Cavium. He is a senior member of the IEEE and ACM.

Yang Xiang received the PhD degree in computer science from Deakin University, Australia. He holds the position of the dean of Digital Research & Innovation Capability Platform, Swinburne University of Technology, Australia. In the past 20 years, he has been working in the broad area of cyber security, which covers network and system security, AI, data analytics, and networking. His translational research has made significant impact to the real-world applications, such as blockchain applications, AI-driven cyber security applications, cloud and IoT security applications. In particular, he is currently leading his team developing active defense systems against large-scale distributed network attacks. He is a senior member of the IEEE.

Yan Zhang received the PhD degree from the School of Electrical & Electronics Engineering, Nanyang Technological University, Singapore. He is full professor with the Department of Informatics, University of Oslo, Norway. He is an associate technical editor of the *IEEE Communications Magazine*, an editor of the *IEEE Network Magazine*, an editor of the *IEEE Transactions on Green Communications and Networking*, an editor of the *IEEE Communications Surveys & Tutorials*, an editor of the *IEEE Internet of Things Journal*, an editor of the *IEEE Vehicular Technology Magazine*, and an associate editor of the *IEEE Access*. He serves as chair positions in a number of conferences, including IEEE GLOBECOM 2017, IEEE VTC-Spring 2017, IEEE PIMRC 2016, IEEE CloudCom 2016, IEEE ICCC 2016, IEEE CCNC 2016, IEEE SmartGridComm 2015, and IEEE CloudCom 2015. He serves as TPC member for numerous international conference including IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, and IEEE WCNC. His current research interests include: next-generation wireless networks leading to 5G, green and secure cyber-physical systems (e.g., smart grid, healthcare, and transport). He is IEEE VTS (Vehicular Technology Society) distinguished lecturer. He is also a senior member of the IEEE, IEEE ComSoc, IEEE CS, IEEE PES, and IEEE VT Society.