Hindawi
Security and Communication Networks
Volume 2019, Article ID 2964673, 2 pages
https://doi.org/10.1155/2019/2964673

Editorial

Security, Privacy, and Trust for Cyberphysical-Social Systems

Laurence T. Yang,[1] **Wei Wang**,[2] **Gregorio Martinez Perez**,[3] **and Willy Susilo**[4]

[1]*Department of Computer Science, St. Francis Xavier University, Canada*
[2]*School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, 430074 Hubei, China*
[3]*Department of Information and Communications Engineering, University of Murcia, Spain*
[4]*School of Computing and Information Technology, University of Wollongong, Australia*

Correspondence should be addressed to Laurence T. Yang; ltyang@stfx.ca

Received 24 December 2018; Accepted 24 December 2018; Published 3 February 2019

A total of 19 manuscripts were received in the final edition of this special issue, and only 8 of these were accepted. This issue covers two frontier topics that are Cyber-Physical-Social Systems (CPSS) and security. This special issue started since we notice that Cyber-Physical-Social Systems (CPSS) include the cyber world, physical world, social world, and their integrations such as the CPS/IoT (the integration of the cyber world and physical world) and the social computing (the integration of the cyber world and the social world), while any of the three suffers tremendous of threats on security. The ultimate goal of CPSS is to provide proactive and personal services for humans. Accordingly, one of the most important concerns of CPSS is to protect sensitive or private data, guarantee user privacy, and ensure the system trustworthy. CPSS security, privacy, and trust as a new research and development field require further development and advances of the corresponding models and methodologies for effective connections among physical, cyber, and social worlds.

The received manuscripts cover all involved worlds in CPSS and most challenging attacks that would meet in CPSS. We selected 8 papers that are well structured, written, and contributive for CPSS security issue.

As the fundamental of CPSS, sensors always act as hardware support that connects data of physical world to human being. However, both security guarantee and energy consumption constrain the developments of sensors in CPSS while privacy data may involve, for example, camera and e-health. C. A. Lara-Nino et al. explore the effects of authenticated encryption to hardware implementation in the physical world phase and accordingly present generic composition of authenticated encryption on FPGA chips, which brings lightweight cryptography with lowered power consumption. Additionally, W. Qiang et al. propose P-CFI, a fine-grained Control-Flow Integrity (CFI) method, to protect CPS against memory-related attacks. They choose points-to analysis to construct the legitimate target set for every indirect call cite and check whether the target of the indirect call cite is in the legitimate target set at runtime.

On an orthogonal direction, J. Hingant et al. introduce HYBINT, an enhanced intelligence system that provides the necessary decision-making support for an efficient critical infrastructures protection by combining the real-time situation of the physical and cyber domains in a single visualization space. HYBINT is a real cross-platform solution which supplies, through Big Data analytical methods and advanced representation techniques, hybrid intelligence information from significant data of both physical and cyber data sources in order to bring an adequate hybrid situational awareness (HSA) of the cyber-physical environment. The HYBINT system consists of three main modules: Data Gathering Modules, Data Analysis Modules, and Data Visualization Module. In another article, Y. Zhu et al. propose an approximate Fast privacy-preserving equality Test Protocol (FTP), which can securely complete string equality test and achieve high running efficiency at the cost of little accuracy loss. They strictly analyze the accuracy of our proposed scheme and formally prove its security. Additionally, they leverage extensive simulation experiments to evaluate the running cost, which confirms its high efficiency.

Z. Ma et al. consider privacy issues related to the social world and construct a personalized and continuous location privacy-preserving framework called GLPP in account linked platforms with different LBSs (Location-Based Services). The framework GLPP obfuscates every location in local search

before submission and performs better than initial protection in accuracy, certainty, and correctness. Meanwhile it can also provide a good user experience without much loss in location utility.

The remaining articles show more interests on cryptographic techniques.

In application layer, data security and privacy are the most serious issues that would raise great concerns from users when they adopt cloud systems to handle data collaboration. However, different cryptographic techniques are deployed in different cloud service providers, which make cross-cloud data collaboration to be a deeper challenge. Q. Huang et al. discuss the challenge and the possible solution based on conditional proxy reencryption and then realize the solution through an adaptive secure cross-cloud data collaboration scheme with identity-based cryptography (IBC) and proxy reencryption (PRE) techniques. The leverage of those cryptographic technologies brings the cyber world in CPSS with data confidentiality and flexible data migration among ciphertexts encrypted in identity-based encryption manner and ciphertexts encrypted in identity-based broadcast encryption manner. Another article concentrates on real-time encrypted transmission for devices in IoT. C. Wang et al. introduce an instant encrypted transmission based security scheme for devices in IoT which guarantees both security and instant responses for IoT data with bilinear pairing and ID-based signature.

There are also researches on Blockchain, a popular topic in security area.

When a popular technology, for instance, Blockchain, involves in CPSS, we definitely wonder sparkles would appear. Will it conquer challenges of security and privacy to IoT entities? Blockchain (BC) technology, which underpins the cryptocurrency Bitcoin, has played an important role in the development of decentralized and data intensive applications running on millions of devices. In this paper, C. Qu et al. propose a framework with layers, intersect, and self-organization Blockchain Structures (BCS) to establish the relationship between IoT and BC for device credibility verification. This new framework demonstrates the validity of the proposed credibility verification method, as well as enhancement in storage expenses and response time.

Therefore, in our opinion, this special issue brings novel and comprehensive insights into the essential techniques for Security, Privacy, and Trust for Cyber-Physical-Social Systems. We hope that this information will contribute to develop CPSS more secure and reliable.

Conflicts of Interest

The editors declare that they have no conflicts of interest regarding the publication of this special issue.

Laurence T. Yang
Wei Wang
Gregorio Martinez Perez
Willy Susilo