Introduction to the Special Issue on User-Centric Security and Safety for CPS

The recent spate of cyber security attacks has reinforced the importance of cyber security. Cyber security is no longer just a technical issue requiring the proficiency and capabilities of technical experts, it is a global phenomenon requiring the attention of stakeholders across different information domains. We organize this special issue on user-centric security and safety aspects of cyber-physical systems (CPS) with the aim of filling gaps between user behaviour and the design of complex CPS. These include different stakeholders' roles and responsibilities, user-centric decision-making capabilities and situational awareness, user experience design, mitigation of user errors and analysing their impact, adaptive risk management, user or operator's trust, security and safety in the device's or system's authentication, access control, and configuration management, hence, the relation to the development of the system's security and safety in the cyber-physical world. It is presumed that alignment of user-oriented processes, standards, and guidelines for security and safety are required to cope with the complexities and interoperability of cyber-physical systems. In other words, this special issue aims to publish the latest advancements in user-centric security and safety techniques and controls for CPS and related components. The following seven contributed articles are included in this special issue:

The first article, entitled "[Efficient Multi-factor User Authentication Protocol with Forward Secrecy for Real-time Data Access in WSNs](#)," proposes a robust multi-factor authentication scheme that makes use of the imbalanced computational nature of the RSA cryptosystem, particularly suitable for scenarios where sensor nodes (but not the user's device) are the main energy bottleneck. This work is the first one that can satisfy all 12 criteria of the state-of-the-art evaluation metric under the harshest adversary model so far.

The second article, entitled "[A Multi-label Fuzzy Relevance Clustering System for Malware Attack Attribution in the Edge Layer of Cyber Physical Networks](#)," proposes a novel multi-label fuzzy clustering system for malware attack attribution. The authors first observed that a multi-label classifier does not classify a part of the samples when classifying malware families. To overcome this problem, the authors developed an ensemble-based multi-label fuzzy classification method to suggest the relevance of a malware instance to the stricken families.

The third article, entitled "[A User-centric Security Solution for Internet of Things and Edge Convergence](#)," proposes a user-centric security solution to ensure the trustworthiness of the data for emergency evaluation in Edge datacenters (EDCs). A user-centric security approach by authenticating users and devices before any communications is established.

The fourth article, entitled "[MobileTrust: Secure Knowledge Integration in VANETs](#)," is about the security of Vehicular Ad hoc NETWORKS (VANET). The authors propose MobileTrust—a hybrid trust-based system for secure resource sharing in VANETs. The proposal utilizes cloud

ACM Reference format:

Neetesh Saxena, Alvaro A. Cardenas, Raheem Beyah, Rongxing Lu, Kim-Kwang Raymond Choo, and Yiran Chen. 2020. Introduction to the Special Issue on User-Centric Security and Safety for CPS. *ACM Trans. Cyber-Phys. Syst.* 4, 3, Article 29 (May 2020), 2 pages.
<https://doi.org/10.1145/3392715>

© 2020 Copyright held by the owner/author(s).

2378-962X/2020/05-ART29

<https://doi.org/10.1145/3392715>

and upcoming 5G technologies to provide robust trust establishment with global scalability. MobileTrust is deployed on a typical embedded system platform and applied on a real smart car installation for monitoring traffic and road-state parameters of an urban application.

The fifth article, entitled “[CirclePIN: A Novel Authentication Mechanism for Smartwatches to Prevent Unauthorized Access to IoT Devices](#),” identifies a unique role of smartwatches as both sensitive data sources and user identity proxies. The authors argue that this new scenario calls for a strengthened and more resilient authentication of users on these devices, and they present an innovative authentication scheme targeted at smartwatches, namely, CirclePIN, that provides both resilience to most common attacks and a high level of usability in tests with real users.

The sixth article, entitled “[HUCDO: A Hybrid User-centric Data Outsourcing Scheme](#),” reveals the need of a hybrid outsourcing model that exploits both cloud server and edge devices to store data for security and efficiency. The authors propose the first hybrid user-centric data outsourcing (HUCDO) scheme, which allows users to outsource data securely, efficiently, and economically via different CPSs. HUCDO offers a secure, efficient, and economical solution for users to implement while outsourcing their data via CPSs.

The last and seventh article, entitled “[A User-centric Approach Toward Resilient Frequency-regulating Wind Generators](#),” investigates how malicious controllable loads can threaten the integrity of frequency-regulating wind generators. Adopting a user-centric approach and benefiting from small-signal analyses, the work shows for the first time how these wind generators can be the target of attackers. The authors modeled and explored how proper tuning and design of the physical system can improve cyber-physical security.

We hope our readers enjoy this special issue!

Neetesh Saxena
Alvaro A. Cardenas
Raheem Beyah
Rongxing Lu
Kim-Kwang Raymond Choo
Yiran Chen

Guest Editors