



Editorial

Security, privacy and trust of user-centric solutions

Raja Naeem Akram^a, Hsiao-Hwa Chen^b, Javier Lopez^c, Damien Sauveron^d, Laurence T. Yang^e

^a Information Security Group Smart Card Centre, Royal Holloway, University of London, Egham, United Kingdom

^b Department of Engineering Science, National Cheng Kung University, Tainan 70101, Taiwan

^c Computer Science Department, University of Malaga, Ada Byron building, 29071 Malaga, Spain

^d XLIM (UMR CNRS 7252 / Université de Limoges), MathIS. Limoges, France

^e Department of Computer Science, St. Francis Xavier University, Antigonish, Canada



ARTICLE INFO

Keywords:

User-centric solutions
Security
Privacy
Trust

ABSTRACT

With the development of pervasive and ubiquitous computing, of IoT and personal devices, user-centric solutions will be the paradigm for most of the future applications. In this context, user-centric solutions must be proposed from deployment models to the content management. Obviously suitable Security, Privacy and Trust (SPT) solutions have to be proposed to ensure the smooth operation of systems and their straightforward managements required for a successful mass-user adoption. In this paper, we summarize the literature related to user-centric SPT scenarios and present a selection of the most recent advances in these areas.

© 2017 Published by Elsevier B.V.

1. Introduction

In future computing environments, due to the ongoing development of pervasive and smart technologies, movement towards user-centric solutions is paramount. The frameworks for everyday personal computing devices, including smartphones and smart cards, are becoming user-centric instead of issuer-centric [1]. User-centric solutions can target a wide range of applications, from individual devices communicating with other connected devices, through to data-sharing in cloud computing and open grids on very powerful computing systems. User-centric solutions address the devices and the ways in which they communicate, i.e. networks and end-user applications. The key factor in the success of user-centric solutions is the convenience for users; to achieve this Security, Privacy and Trust (SPT) in the user-centric ecosystem for any device must be ensured.

Until now, very few pieces of work related to user-centric SPT have been published in various journals and conferences; to cite a few in different domains:

- Castiglione et al. [2] propose secure group communication schemes in user-centric networks. They focus their attention on key predistribution for secure communications in those networks and introduce Multi-PRSA, a novel scheme which efficiently extends and improves Polynomial Predistribution Random Subset Assignment Scheme (PRSA), in order to increase resilience against collusion attacks.
- De las Cuevas et al. [3] introduce a novel self-adaptive user-centric end-to-end system, named Multi-platform Usable

Endpoint Security (MUSES) to securely manage Bring Your Own Device (BYOD) environment. MUSES considers users behavior in order to adapt, improve, and even increase the defined set of security rules. To do this, the system applies Machine Learning and Computational Intelligence techniques, being also able to predict future security incidents produced by these users.

- Gubbi et al. [4] present a user-centric cloud centric vision for worldwide implementation of Internet of Things in which associated challenges have been highlighted ranging from appropriate interpretation and visualization of the vast amounts of data, through to the privacy, security and data management issues that must underpin such a platform in order for it to be genuinely viable.
- Sánchez-García et al. [5] propose On-SiteDriverID, a secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks, which has a user-centric design for road authorities point of view. They have conducted an evaluation of the proposal on simulated realistic VANET urban scenarios over a map of the city of Barcelona.
- Akram et al. [6] discuss two of the most widely accepted and deployed smart card management architectures in the smart card industry: GlobalPlatform and Multos and explain how these architectures do not fully comply with the User Centric Smart Card Ownership Model (UCOM) and GlobalPlatform Consumer-Centric Model (GP-CCM). They then design a novel flexible consumer-centric card management architecture designed specifically for the UCOM

and GP-CCM frameworks, along with ways of integrating the Trusted Service Manager (TSM) model into the proposed card management architecture whilst addressing the potential security issues.

- Vossaert et al. [7] present a user-centric identity management using trusted modules that tackles several privacy and security problems of current federated identity management systems (FIMs) and also adds extra functionality.
- Henze et al. [8] present User-driven Privacy Enforcement for Cloud-based Services in the IoT (UPECSI), a solution which takes a comprehensive approach to privacy for the cloud-based IoT by providing an integrated solution for privacy enforcements that focuses on individual end-users and developers of cloud services at the same time. UPECSI enables individual end-users to protect their potentially sensitive data before it is transferred to the cloud; empowers cloud service developers to efficiently integrate privacy functionality into the development process of a cloud service; and provides users an intuitive, adaptable, and transparent user interface which allows them to configure their privacy settings based on their individual privacy experience.
- Suriadi et al. [9] propose an extension of the existing federated single sign-on (FSSO) systems that adopts the beneficial properties of the user-centric identity management (UCIM) model. This new identity management system allows the users to control and enforce their privacy requirements while still retaining the convenience of single sign-on over a federation of service providers.
- Schreckling et al. [10] introduce Kynoid, a real-time monitoring and enforcement framework for Android. It is based on user-defined security policies which are defined for data-items. This allows users to define temporal, spatial, and destination constraints which have to hold for single items.
- Jin et al. [11] propose a unified access control scheme that supports patient-centric selective sharing of virtual composite Electronic Health Records (EHRs) using different levels of granularity, accommodating data aggregation and privacy protection requirements.
- Frangoudis et al. [12] focus on the provision of secure, user-centric voice services and explore their potential performance-wise, by designing a VoIP communications scheme tailored to open-access wireless environments.

The aims of this special issue being to gather and foster researches on this key topic of user-centric solutions, authors have been invited to submit original research papers on the state of the art, latest results and advances in SPT solutions for user-centric devices, network and applications, highlighting trends and challenges. Topics of this special issue included:

- Security, Privacy and Trust of:
 - User-centric Devices (Smartphones, PDA, RFID, Sensors, Smart Cards, Smart Cameras, Smart Objects),
 - User-centric Networks (Mobile Ad hoc Networks, M2M Networks, Urban Networks, Wireless Sensor Networks),
 - User-centric Applications (Cloud Computing, Data Provenance, Smart Grids, Smart Homes, Healthcare, Smart Spaces, Convergent Pervasive and Smart Environments);
- Technologies used to enhance Security, Privacy and Trust in User-centric solutions (NFC, IPv6, TPM);
- Societal issues related to Security, Privacy and Trust in User-centric solutions (HCI, User interactions).

After a rigorous review process, among the 73 very high quality submissions received, only 18 papers have been accepted for publication in this issue.

2. Content of this issue

In this special issue, the accepted papers are either related to domains of application, like finance or healthcare, either they are dealing with malware detection and security of mobile applications. Some selected papers are related to users' privacy or to secure resource/data-sharing solutions whereas few others address miscellaneous close topics.

2.1. SPT in financial domain

The first paper, "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry" by Qiu et al. [13] proposes an approach to proactively protect financial customers privacy information using Attributed-Based Access Control (ABAC) as well as data self-deterministic scheme.

The second paper, "Evaluation of transaction authentication methods for online banking" by Kiljan et al. [14] studies the online banking authentications in a user-centric context and proposes to extend an existing mechanism which quantifies accessibility, memorability, security and vulnerability characteristics, with aspects related to the feasibility dimension of secure usability of transaction authentication methods.

The third paper, "Secure and anonymous decentralized Bitcoin mixing" by Ziegeldorf et al. [15] proposes CoinParty, an efficient decentralized mixing service that allows users to reestablish their financial privacy in Bitcoin and related cryptocurrencies. Through a novel combination of decryption mixnets with threshold signatures, CoinParty takes a unique place in the design space of mixing services, combining the advantages of previously proposed centralized and decentralized mixing services in one system.

2.2. SPT in healthcare domain

The fourth paper, "On the design and analysis of protocols for Personal Health Record storage on Personal Data Server devices" by Belyaev et al. [16] proposes a new architecture, namely Personal Data Server (PDS) overlay, where the electronic Personal Health Records (PHRs) data is stored on a set of Secure Portable Tokens (SPTs, *i.e.* cheap, portable, and secure devices combining the computing power and tamper-resistant properties of the smart cards and the storage capacity of NAND flash memory chips and being able to act as a PDS) that are under the control of individual users. A formal analysis is also provided to ensure the correct behavior of the protocols used in PDS overlays.

The fifth paper, "A robust and anonymous patient monitoring system using wireless medical sensor networks" by Amin et al. [17] proposes an architecture for patient monitoring healthcare system in wireless medical sensor networks and designs an anonymity-preserving mutual authentication protocol for mobile users. The AVISPA tool is used to simulate the proposed protocol and demonstrates it resists the existing well known attacks.

2.3. SPT for malware detection and mobile applications

The sixth paper, "Owner based malware discrimination" by Han et al. [18] introduces the relativity issue of discrimination technique and proposes a malicious software discrimination model, named as Unlimited Register Machine of Owners (URMO) which includes analyzing and defining operations and objects as two elements of discrimination, introducing the concept of owner to give a reference to malicious signature, and comparing the model of Unlimited Register Machine (URM) with URMO to explain the origin of false positive and false negative.

Download English Version:

<https://daneshyari.com/en/article/6873337>

Download Persian Version:

<https://daneshyari.com/article/6873337>

[Daneshyari.com](https://daneshyari.com)