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*

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.

Keywords: User-centric Solutions, Security, Privacy, Trust

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 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 incidences 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 health-care 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.

The seventh paper, "Risk analysis of Android applications: A user-centric solution" by Dini *et al.* [19] presents a framework, called Multi-criteria App Evaluator of TRust for AndrOID (MAETROID), to evaluate the trustworthiness of Android apps by performing a multi-criteria analysis of an app at deploy-time and returning a single easy-to-understand evaluation of the apps risk level (*i.e.*, Trusted, Medium Risk, and High Risk) to help the user deciding on whether or not installing a new app.

The eighth paper, "Automatic security verification of mobile app configurations" by Costa *et al.* [20] proposes a novel technique for the security verification of groups of mobile app whose the approach relies on partial model checking (PMC) to extend the existing security guarantees to groups of applications.

The ninth paper, "You can't touch this: Consumer-centric android application repackaging detection" by Gurulian *et al.* [21] proposes an approach for detecting repackaged applications by taking advantage of the attackers reluctance to significantly alter the elements that characterise an application without notably impacting the applications distribution.

2.4. SPT for users' privacy

The tenth paper, "Your WiFi is leaking: What do your mobile apps gossip about you?" by Atkinson *et al.* [22] describes how mobile device apps can inadvertently broadcast personal information through their use of wireless networks despite the correct use of encryption and they present a remote, undetectable, detection mechanism to infer private user information through observation of encrypted app network activity.

The eleventh paper, "Time-based low emission zones preserving drivers privacy" by Jardí-Cedó *et al.* [23] presents a new user-centric Electronic Road Pricing (ERP) system for Low-Emission Zones (LEZs) that preserves the privacy of honest drivers and that is able to detect fraudulent drivers and revoke their anonymity.

2.5. SPT for resource/data-sharing solutions

The twelfth paper, “XSACd-Cross-domain resource sharing & access control for smart environments” by Fysarakis *et al.* [24] presents XSACd, a cross-domain resource sharing and access control framework for smart environments, combining the well-studied fine-grained access control provided by the eXtensible Access Control Markup Language (XACML) with the benefits of Service Oriented Architectures, through the use of the Devices Profile for Web Services (DPWS). Based on standardized technologies, this framework enables seamless interactions and fine-grained policy-based management of heterogeneous smart devices, including support for communication between distributed networks, via the associated MQ Telemetry Transport protocol (MQTT) based proxies.

The thirteenth paper, “AFT: Adaptive and fault tolerant peer-to-peer overlay - A user-centric solution for data sharing” by Poenaru *et al.* [25] proposes AFT, an overlay that adapts to a changing number of nodes, which is resilient to faults and the foundation for an efficient implementation of a reputation based trust system. The AFT overlay is designed to be a solution for systems that need to share transient information, performing a synchronization between various components, like in mobile ad-hoc networks, M2M networks, urban networks, and wireless sensor networks.

2.6. Miscellaneous SPT of user-centric solutions

The fourteenth paper, “Trusted mobile computing: An overview of existing solutions” by Bouazzouni *et al.* [26] presents a comprehensive surveys of the hardware-based (Secure Elements, Trusted Platform Module and Trusted Execution Environments) and software-based (Virtualization Environments) solutions for trusted mobile computing.

The fifteenth paper, “A Sybil attack detection scheme for a forest wildfire monitoring application” by Jan *et al.* [27] proposes two different techniques for Sybil attack detection for a forest wildfire monitoring application. The first one is a two-tier detection technique which uses high-energy nodes operating at a lower level to detect forged identities of Sybil nodes. The second one is a residual energy-based detection technique which uses the residual energy of each node to detect a possible Sybil attack at the high energy nodes.

The sixteenth paper, “HB$^+$DB: Distance bounding meets human based authentication” by Pagnin *et al.* [28] proposes to mitigate the man-in-the-middle attack against HB+ protocol by using physical layer measures from distance-bounding protocols and simple modifications to devices radio receivers.

The seventeenth paper, “Full integrity and freshness for cloud data” by Jin *et al.* [29] presents the design, implementation and evaluation of such a secure storage system where confidentiality, full integrity and instantaneous freshness check are achieved.

The eighteenth paper, “A novel face recognition algorithm via weighted kernel sparse representation” by Liu *et al.* [30] proposes a novel face recognition algorithm called Weighted Kernel Sparse Representation based Classification (WKSRC) whose experiments on the AR database reveal, it is more effective than SRC, WSRC and KSRC in term of recognition accuracy and, especially, it has better ability to deal with the occlusion scene.

3. Conclusion

Security, privacy and trust in many aspects cannot be envisioned as solely technical problems. Individual users that interact with the modern technology, have to taken in as equal partners to build a holistic system that provides foolproof security, privacy and trust mechanisms. Therefore, there is an emerging trend in the technology sphere especially and information security particularly, of developing technical solutions that involve, and empower its users. This trend has the potential to solve not only the present challenges but also the future challenges posed by emerging technologies like IoT, autonomous systems (transports, cars, drones) and Artificial Intelligence (AI). This paper has charted a small sample of this trend and its potential for the future.

Acknowledgments

We would like to thank all authors who submitted their papers, and all the reviewers for their time and effort. Their thorough reviews and valuable comments enabled us to select the papers, and provide a high quality Special Issue. We would also like to thank the FGCS Editor-in-Chief, Professor Peter Sloot, and the Elsevier staff for their help and support that made this Special Issue possible. We hope this Special Issue will serve as a reference for many future research projects.

References

[1] R. N. Akram, K. Markantonakis, K. Mayes, A Paradigm Shift in Smart Card Ownership Model, in: Computational Science and Its Applications (ICCSA), 2010 International Conference on, pp. 191–200.

[2] A. Castiglione, P. D'Arco, A. D. Santis, R. Russo, Secure group communication schemes for dynamic heterogeneous distributed computing, Future Generation Computer Systems (2015) –.

[3] P. de las Cuevas and A.M. Mora and J.J. Merelo and P.A. Castillo and P. García-Sánchez and A. Fernández-Ares, Corporate security solutions for BYOD: A novel user-centric and self-adaptive system, Computer Communications 68 (2015) 83 – 95. Security and Privacy in Unified Communications: Challenges and Solutions.

[4] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems 29 (2013) 1645 – 1660. Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services & Cloud Computing and Scientific Applications Big Data, Scalable Analytics, and Beyond.

[5] J. Sánchez-García and J.M. García-Campos and D.G. Reina and S.L. Toral and F. Barrero, On-siteDriverID: A secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks, Future Generation Computer Systems 64 (2016) 50 – 60.

[6] R. N. Akram, K. Markantonakis, D. Sauveron, A novel consumer-centric card management architecture and potential security issues, Information Sciences 321 (2015) 150 – 161. Security and privacy information technologies and applications for wireless pervasive computing environments.

[7] J. Vossaert, J. Lapon, B. D. Decker, V. Naessens, User-centric identity management using trusted modules, Mathematical and Computer Modelling 57 (2013) 1592 – 1605. Public Key Services and Infrastructures EUROPKI-2010-Mathematical Modelling in Engineering & Human Behaviour 2011.

[8] Martin Henze and Lars Hermerschmidt and Daniel Kerpen and Roger Häußling and Bernhard Rumpe and Klaus Wehrle, A comprehensive approach to privacy in the cloud-based Internet of Things, Future Generation Computer Systems 56 (2016) 701 – 718.

[9] S. Suriadi, E. Foo, A. Jøsang, A user-centric federated single sign-on system, Journal of Network and Computer Applications 32 (2009) 388 – 401.

[10] D. Schreckling, J. Köstler, M. Schaff, Kynoid: Real-time enforcement of fine-grained, user-defined, and data-centric security policies for Android, Information Security Technical Report 17 (2013) 71 – 80. Security and Privacy for Digital Ecosystems.

[11] J. Jin, G.-J. Ahn, H. Hu, M. J. Covington, X. Zhang, Patient-centric authorization framework for electronic healthcare services, Computers & Security 30 (2011) 116 – 127. Special Issue on Access Control Methods and Technologies.

[12] P. A. Frangoudis, G. C. Polyzos, On the performance of secure user-centric VoIP communication, Computer Networks 70 (2014) 330 – 344.

[13] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, H. Zhao, Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry, Future Generation Computer Systems (2016) –.

[14] S. Kiljan, H. Vranken, M. van Eekelen, Evaluation of transaction authentication methods for online banking, Future Generation Computer Systems (2016) –.

[15] J. H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, K. Wehrle, Secure and anonymous decentralized Bitcoin mixing, Future Generation Computer Systems (2016) –.

[16] K. Belyaev, W. Sun, I. Ray, I. Ray, On the design and analysis of protocols for Personal Health Record storage on Personal Data Server devices, Future Generation Computer Systems (2016) –.

[17] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, N. Kumar, A robust and anonymous patient monitoring system using wireless medical sensor networks, Future Generation Computer Systems (2016) –.

[18] L. Han, S. Liu, S. Han, W. Jia, J. Lei, Owner based malware discrimination, Future Generation Computer Systems (2016) –.

[19] G. Dini, F. Martinelli, I. Matteucci, M. Petrocchi, A. Saracino, D. Sgandurra, Risk analysis of Android applications: A user-centric solution, Future Generation Computer Systems (2016) –.

[20] G. Costa, A. Merlo, L. Verderame, A. Armando, Automatic security verification of mobile app configurations, Future Generation Computer Systems (2016) –.

[21] I. Gurulian, K. Markantonakis, L. Cavallaro, K. Mayes, You can't touch this: Consumer-centric android application repackaging detection, Future Generation Computer Systems 65 (2016) 1 – 9. Special Issue on Big Data in the Cloud.

[22] J. S. Atkinson, J. E. Mitchell, M. Rio, G. Matich, Your WiFi is leaking: What do your mobile apps gossip about you?, Future Generation Computer Systems (2016) –.

[23] R. Jardí-Cedó, M. Mut-Puigserver, M. M. Payeras-Capellà, J. Castellà-Roca, A. Viejo, Time-based low emission zones preserving drivers' privacy, Future Generation Computer Systems (2016) –.

[24] K. Fysarakis, O. Soultatos, C. Manifavas, I. Papaefstathiou, I. Askoxylakis, XSACd-Cross-domain resource sharing & access control for smart environments, Future Generation Computer Systems (2016) –.

[25] A. Poenaru, R. Istrate, F. Pop, AFT: Adaptive and fault tolerant peer-to-peer overlay - A user-centric solution for data sharing, Future Generation Computer Systems (2016) –.

[26] M. A. Bouazzouni, E. Conchon, F. Peyrard, Trusted mobile computing: An overview of existing solutions, Future Generation Computer Systems (2016) –.

[27] M. A. Jan, P. Nanda, X. He, R. P. Liu, A Sybil attack detection scheme for a forest wildfire monitoring application, Future Generation Computer Systems (2016) –.

[28] E. Pagnin, A. Yang, Q. Hu, G. Hancke, A. Mitrokotsa, HB$^+$DB: Distance bounding meets human based authentication, Future Generation Computer Systems (2016) –.

[29] H. Jin, K. Zhou, H. Jiang, D. Lei, R. Wei, C. Li, Full integrity and freshness for cloud data, Future Generation Computer Systems (2016) –.

[30] X. Liu, L. Lu, Z. Shen, K. Lu, A novel face recognition algorithm via weighted kernel sparse representation, Future Generation Computer Systems (2016) –.