Internet of People, Things and Services - The Convergence of Security, Trust and Privacy

JHP Eloff[1,3,4], MM Eloff[2], MT Dlamini[1,3,4], MP Zielinski[1,3,4]

[1]Information and Computer Security Architectures Research Group
Department of Computer Science, University of Pretoria, South Africa
[2]School of Computing, UNISA, Pretoria, South Africa
[3]SAP Meraka UTD, CSIR, Pretoria, South Africa
[4]SAP Research CEC Pretoria
[1,3,4]{eloff, mdlamini, zielinski}@cs.up.ac.za; [1,3,4]{jan.eloff, moses.dlamini, marek.zielinski}@sap.com;
[2]eloffmm@unisa.ac.za

Abstract. The Future Internet will consist of billions of people, things and services having the potential to interact with each other and their environment. This highly interconnected global network structure presents new types of challenges from a security, trust and privacy perspective. An example of such a challenge is the handling of an access request to obtain a blood pressure reading: from a monitor (thing) attached to a person (people); supported by a mobile health clinic (service). Furthermore, the patient may request that his/her health data should exclude his/her biographical details and may be released only to trustable health organizations. The IoPTS(security,trust,privacy) structure presented in this paper is a first attempt in simplifying this complex integration of security, trust and privacy issues.

Keywords: Security, Trust, Privacy, Internet, People, Things, Services

1 Introduction

The Future Internet will consist of billions of digital devices, people, services and other physical objects having the potential to seamlessly connect, interact and exchange information about themselves and their environment [1]. In the envisaged Future Internet, people will utilize these digital devices and physical objects to produce and consume web-based services in a web-based service industry [2, 3] in what we refer to as the Internet of People, Things and Services (IoPTS). The envisaged IoPTS consists of three visions i.e. Internet of People (IoP) [4, 3], Internet of Things (IoT) [2] and the Internet of Services (IoS) [3].

The Internet of People is envisaged as a world where people equipped with human-implantable RFID tags will become part of the ubiquitous network of networks facilitated by the popularity of social networks [4, 3]. The ITU envisaged the Internet of Things as a world where physical and digital objects are seamlessly integrated into the Internet to become active participants in business processes [5]. The Internet of Things can also be seen as the integration between the logical and physical word.

Internet of Services is defined as “the vision for next-generation services provided over the Internet” [3].

This paper defines the Internet of People, Things and Services (IoPTS) as the vision where people, things (physical objects) and services are seamlessly integrated into the networks of networks as active participants that exchange data about themselves and their perceived surrounding environments over a web-based infrastructure. The IoPTS, amongst many other aspects, is characterized by: its massivity in terms of people, services, and things, that will generate information populating massive databases; its advanced capability for tracking people, objects and things; its focus is on multiple frontiers, a person can assume multiple identities where each identity is associated with multiple things (devices) connected to multiple services; its vertical mobility with a phenomenal increase in the level of complexity from a governance point of view.

The developed world as well as the developing world will benefit from the IoPTS. The plethora of benefits that society, especially so in the developed world, seeks to gain once the vision of the IoPTS becomes reality, amongst others, include the following: increasing efficiency in material handling and general logistics, product tracking, reducing production and handling costs, speeding the flow of assets, anti-theft and quicker recovery of stolen items [5, 4]. Considering the developing world it is aspects such as mobile health for remote rural areas that will become a reality with the IoPTS. With all these benefits, what stands in the way of achieving the vision of the IoPTS? How do we govern and regulate the players on the IoPTS infrastructure that knows no boundaries? Unlimited personal, thing and service content distribution brings along the issues of trust and privacy. What security measures are required to protect content authenticity, legality of content, legality of possession of such content, non-repudiation and accountability?

Current approaches will fall short in providing trustworthy infrastructures that ensures secure protection of the data and privacy for personally identifiable information of individuals in the era of IoPTS [4]. The envisaged IoPTS requires a very strong foundation with security, trust and privacy as a top priority. Security, trust and privacy should be implemented at design time with the flexibility to adapt, if not automatically, during run time.

Dr Stefan Wess quoted in [3] argues that in order to meet the challenges there is a need to successfully integrate the IoT, IoS, IoP and Internet of Data (IoD). However, there is no mention of how this integration could be done. According to the authors, the paper at hand is a first attempt to build on Wess’s assertion by suggesting a possible way to integrate the IoP, IoS and IoT. The hypothesis postulated in this paper is that the foundation for the successful realization of the IoPTS is a convergence of security, trust and privacy.

The remainder of the paper is structured as follows: Section 2, 3 and 4 discusses security, trust and privacy respectively with the aim in identifying the underlying services for each that can have an impact on creating a trustworthy IoPTS. Section 5 proposes a framework in the form of a cube to be used for the convergence of IoPTS. Section 6 discusses a use case to illustrate the proposed framework. Section 7 concludes the paper.

2 Security and the IoPTS

From the three concepts i.e. Security, Trust and Privacy, security is the most established and implemented as it originated from earlier ICT infrastructures such as mainframes. However, security in the context of the IoPTS is still a very important concept and the basic security services that originally applied to traditional environments are still applicable in the IoPTS.

According to the ISO 7498-2 standard [6], produced by The International Standards Organisation (ISO) Information Security can be defined in terms of:

- Identification & authentication The identification and authentication of any person, thing or service requiring access to another person, thing or service or to a combination of (person, thing, service) is the first step towards injecting security into the IoPTS. More focus needs to be placed on the IoT layer as device identification and authentication is still a maturing technology. Current approaches focusing on identity management will also have to address also things and services.
- Authorisation. The next step towards enforcing Information Security (IS) in the IoPTS is to determine if the authenticated thing, person or service has the right to obtain access. In terms of the authorisation process, control is, therefore, exerted over the access rights of all authenticated things, persons and services. Furthermore issues such as location and context will play an important role in providing authorization as a security service in the IoPTS. It is envisaged that access mechanisms such as user control (UCON), optimistic based access control, variations of RBAC, location and direction based access control and conflict based access control will require serious attention in IoPTS.
- Confidentiality; All information must be strictly accessible to authorised things, persons and services only. Protecting the confidentiality of information, personal and physical objects therefore, gives the assurance that only authorised things, persons and services will have access to the information in question.
- Integrity. Within the IoPTS context information regarding things, persons and services should not only be kept confidential, but its integrity should also be guaranteed.
- Non-repudiation. The last step towards enforcing IS is to ensure that no action performed to affect IS, for example, changing the content of a chunk of information or changing the status of a device (thing), could be denied at a later stage.
- Availability refers to the basic assumption that the right thing, person (information) and service will only be available to the right thing, person or service at the right time [7].

3 Trust and the IoPTS

Trust is increasingly playing an important role in modern ICT infrastructures and will more so be the case in IoPTS. Trust is in principle a human action.

The following concepts relate to trust formation [8] in the context of IoPTS, but this list is not exhaustive:

- Beliefs are related to trust and refer to the acceptance that something is true or real, it is often underpinned by a sense of certainty; a statement, principle, or doctrine that is accepted as true [9]. For example in the IoPTS, should a device be a certified device evaluated by a credible institution it can be postulated that persons and/ or services will have trust (belief) in that device e.g. a thing such as a blood pressure monitor.
- Reputation is the average experiences of trusters over a specific period of time [10, 11]. In the IoPTS the number of successful interactions between for example a thing such as a heart monitor device and a service such as an eHealth service can be used to describe the trust level between the thing and the service. Reputation will play a vital role in the IoPTS especially in the linkage between IoP and IoS.
- Recommendation is essentially the same as reputation as it is based on the truster's experiences with and beliefs regarding the trustee, but the truster will only make the trustworthiness of the trustee known on request [12]. Persons in the IoP context will rely on recommendations from credible bodies to utilize available services.
- A credential is a property or token issued by a trusted third party to the trustee that the trustee can present as proof of his trustworthiness to the truster. It is also referred to as authoritative trust as the credentials can be validated as it was supposed to have been issued by the trusted third party [10]. Similar to current ICT infrastructures, the exchange of certificates (X.509 look a-likes) will have to play an important role in the alignment of the IoT layer with the IoS layer.
- Delegation. When one party transfers the trustworthiness of the trustee to another party, it is termed delegation trust [13]. It is especially the IoP with special reference to the security requirements of Social Networks that will reply on delegation as a mechanism for establishing trust.

4 Privacy and the IoPTS

IoPTS demands new perspectives on the concept of Privacy. However, the paper published in 1890 by Warren and Brandeis [21] provides a definition that stood the test of time. They define privacy as "the right to be let alone". When juxtaposing this against the IoPTS, the concept of privacy needs to be broadened thereby including not only personal privacy but also information privacy and physical privacy.

In the eHealth environment a patient might, for example, be carrying with him/her a biosignals device such as a blood pressure monitor being part of IoTs. From a privacy perspective the patient information, which ends up in an electronic patient

record system on the IoS layer, is to be considered as private. The patient might also prefer that the physical device being part of IoT is not visible to other people and therefore needs not to infringe on his personal/physical privacy.

In the context of IoPTS, personal information and physical privacy are all of importance. Physical privacy is dominant on the IoT layer, whilst personal and information privacy dominantly belong to the IoS and IoP layers. Information privacy has various dimensions, depending on whose privacy we wish to protect [14, 15]. The following concepts relate to privacy in the context of IoPTS, but this is not an exhaustive list:

- Respondent privacy, which focuses on the prevention of re-identification and disclosure of confidential data of respondents. Respondent privacy is usually sought when data is made available by the data owner (i.e. the one that collects the data) to data users. Responded privacy will play a critical role on the IoS layer where massive databases will be populated with information that is linked to people on the IoP layer. It is envisaged that new high-speed personal anonymisation mechanisms will be required to meet the needs of IoPTS.
- Owner privacy, which concentrates on preventing the disclosure of data in a database when two or more autonomous entities wish to compute queries across their databases, such that only the results of the query is revealed. It is usually the goal of privacy-preserving data mining [16, 17, 18]. Data mining activities on the IoS and IoP layers will receive increasing attention resulting in high vulnerability for massive tracker attack threats [7] where aggregated data is involved.
- User privacy, which aims to protect the privacy of queries to interactive databases, in order to prevent user profiling and re-identification [19] [20]. The envisaged tight coupling between the IoP and IoS layers demands advanced tools in minimizing this vulnerability. Search engines in IoPTS will have to provide this.
- Ethical conduct needs to be considered. For example, the IoS layer should take cognizance of requirements regarding ethics and privacy as suggested by world organizations such as the OECD.
- Legal obligations also need to be considered. IoPTS will accelerate the demand for new privacy technologies that are sensitive for differences in international legal systems e.g. the difference regarding the collection of personal information between the USA and the EU

5 IoPTS(security,trust,privacy)

It is clear from the introduction paragraph as well as from the individual discussions on security, trust and privacy, that only an integrated and interrelated perspective on (security, trust, privacy) can potentially deliver an input in the quest to address protection issues in the IoPTS. It is for this reason that the authors of this paper have chosen a cube structure as a modeling mechanism for security, trust and privacy in the IoPTS, referred to as IoPTS(securirty, trust, privacy). A cube has three dimensions with the ability to clearly show the intersection thereof. Therefore a cube is an ideal

modeling structure for depicting the convergence of security, trust and privacy for the IoPTS. The cube (framework) presented in figure 1 is a first attempt in simplifying this complex convergence of security, trust and privacy within the context of the IoPTS.

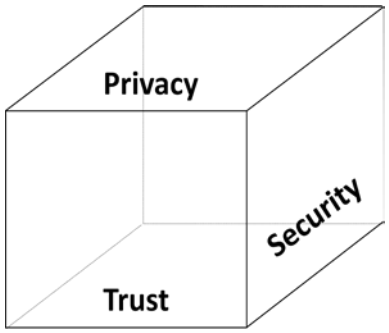

Fig 1 IoPTS(security,trust,privacy)

6. Use case for IoPTS(security,trust,privacy) – a case of handling an access request

Most existing access control models designed for the pre-IoPTS era evaluates access requests based on ($Subject_i$, $Object_i$, $Action_i$) tuples. Existing approaches do not have the ability to handle the high level of complexity required by IoPTS as they were designed to focus on security only, as opposed to the convergence between security, trust and privacy. In IoPTS access information, required to grant/reject access requests, is not only complex but also composite in nature. This is a direct result of the high level of interconnectedness between things, services and people. To illustrate, consider the following use case: How do we define the access information required to grant/reject a request for obtaining a blood pressure measurement from a monitor (IoT) attached to a person (IoP) who is supported through a mobile health service (IoS)? Furthermore the person, being a member of a patient social network (IoP), has agreed to release his/her health related data, stored on the social network, to trustable health organizations affiliated with the World Health Organisation. However, based on the principle of respondent privacy, the person does not want to release any personal information such as name and address. It is clear that the type and structure of information required to grant/reject such an access request is complex and should address the following IoPTS(Security,trust,privacy) issues: security(authorization), trust(reputation), privacy(respondent). This is depicted in figure 2.

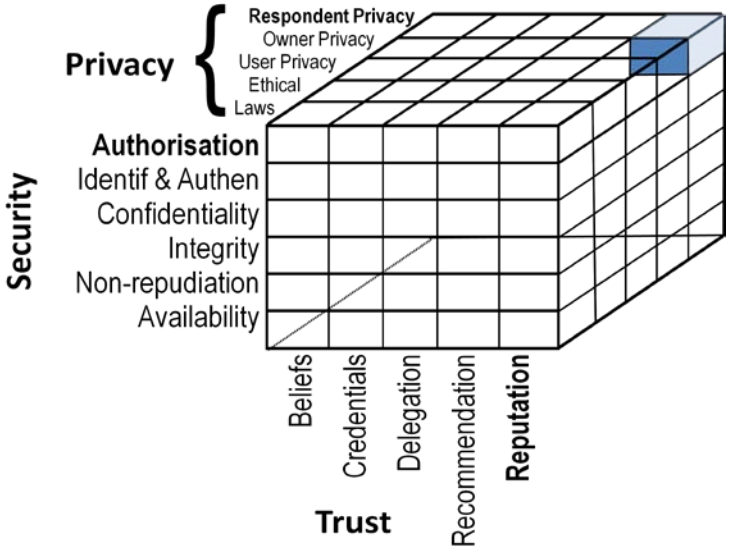

Fig. 2. IoPTS(security(authorization), trust(reputation), privacy(respondent)

7 Conclusion

The IoPTS(security, trust, privacy) structure presents a first attempt in simplifying the complex nature of injecting the necessary protection into the IoPTS. A brief use case with specific reference to handling an access request demonstrated the use of the cube as a modeling structure. However, future work must focus on refining the different aspects of each dimension (security, trust, privacy) of the cube and then focus on the identification of the required mechanisms (intersections of the different dimensions) required by the IoPTS.

Acknowledgments. The support of SAP Research CEC Pretoria/SAP Meraka UTD towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are solely those of the authors and cannot necessarily be attributed to SAP Research CEC Pretoria/SAP Meraka UTD.

References

1. Dlamini, M T, Eloff, M M and Eloff, J H P, Internet of Things: Emerging and Future Scenarios from an Information Security Perspective. Proceedings of SATNAC 2009: Convergence - 21st Century Lifestyle Enabler, 2009.

2. SAP AG. Towards a European Strategy for the Future Internet: A call for Action. [Online] 2009. [Cited: November 14, 2009.] http://www.europeansoftware.org/documents/SAP_WP_FutureInternet.pdf.
3. Heuser, L, Alsdorf, C and Woods, D. International Research Forum 2008. 2009.
4. Kerr, I. The internet of people: Reflections on the Future Regulation of Human-Implantable Radio Frequency Identification. http://www.idtrail.org/. [Online] n.d. [Cited: November 2009, 2009.] http://www.idtrail.org/files/9780195372472_kerr_19.pdf,.
5. ITU Strategy and Policy Unit (SPU),The Internet of Things Executive Summary. www.itu.int/. [Online] 2005. [Cited: November 27, 2008.] www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf.
6. ISO. ISO 7498-2:1989. Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture. Geneva: ISO, 1989. ISO 7498-2.
7. Pleeger, C P and Pfleeger, S L. Security in Computing. Upper Saddle River : Prentice Hall, 2007.
8. Oxford English Dictionary. [Online] 2009. [Cited: 11 10, 2009.] www.oed.com.
9. Encarta ® World English Dictionary ©. s.l. : Microsoft Corporation, Developed for Microsoft by Bloomsbury Publishing Plc. (1999), 1999.
10. Dragovic, B., Hand, H., Harris, T., Kotsovinos, E., and Twigg, A. Managing Trust and Reputation in the XenoServer Open Platform. A., P. Nixon and S. Terzis [ed.] LNCS 2692, 2003. Trust Management 2003. pp. 59-74.
11. Kinateder, M and Rothermel, K. Architecture and Algorithms for Distributed Reputation Systems. P. Nixon & S. Terzis. [ed.] LNCS 2692, 2003. Trust Management 2003. pp. 1-16.
12. Abdul-Rahman, A and Hailes, S. A Distributed Trust Model.. New Security Paradigms Workshop Langdale, Cumbria UK, available online at http://portal.acm.org/ft_gateway.cfm?id=283739&type=pdf&dl=GUIDE&dl=ACM&CFID=111111. 1997
13. Jøsang, A, Ismail, R and Boyd, C. A Survey of Trust and Reputation Systems for Online Service Provision. Decision Support Systems, Vol. 43, pp. 618-644. 2007
14. Domingo-Ferrer, J and Saygin, Y. Recent progress in database privacy. Data and Knowledge Engineering, Vol. 68, pp. 1157-1159. 11, November 2009.
15. Domingo-Ferrer, J. A three-dimensional conceptual framework for database privacy. In Secure Data Management-4th VLDB Workshop SDM'2007. 2007.
16. Emekci, F., Sahin, O. D., Agrawal, D., & Abbadi, A. E. Privacy preserving decision tree learning over multiple parties. 2, Data and Knowledge Engineering, Vol. 63, pp. 348-361. 2007.
17. Agrawal, D and Aggarwal, C C. On the design and quantification of privacy preserving data mining algorithms. Santa Barbara: In Proceedings of the twentieth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems. pp. 247-255. 2001.
18. Clifton, C, Kantarcioglu, M and Vaidya, J. Privacy-preserving data mining. [ed.] W W Chu and T Y Lin: Springer-Verlag. Foundations and Advances in Data Mining, pp. 313-344. 2005.
19. Chor, B., Kushilevitz, E., Goldreich, O. and Sudan, M. Private information retrieval. Journal of the ACM, Vol. 45(6), pp. 965-981. 1998.
20. Domingo-Ferrer, J. Bras-Amoros, M., Wu, Q., & Manjon, J. User-private information retrieval based on a peer-to-peer community. Data and Knowledge Engineering, Vol. 68, pp. 1237-1252. 2009.
21. Warren, S., & Brandeis, L. (1890). The right to privacy. Harvard Law Review, 14(5), 193 - 220.