The Relationship Between Privacy, Information Security and the Trustworthiness of a Crowdsourcing System in a Smart City

L. Cilliers and S. Flowerday

University of Fort Hare, South Africa
lcilliers@ufh.ac.za; sflowerday@ufh.ac.za

Abstract

With the growing number of people living in cities, the challenges faced by governments in providing an acceptable standard of service delivery are immense. 'Smart cities' is a new and innovative approach that has been formulated over the past few years in order to use current infrastructure and resources more effectively and efficiently. For a smart city to work, large amounts of information must be collected from the citizens, which may cause privacy concerns. Information security influences the perceived trustworthiness of the crowdsourcing system which, in turn, increases the participation of citizens in smart city projects. This paper investigates the relationship between the privacy, information security and perceived trustworthiness of a crowdsourcing system in a smart city. The study made use of a quantitative approach using a survey design. A questionnaire was completed by 361 participants in a public safety project hosted in East London, South Africa. The results indicated there is a positive relationship between the information security in and the perceived trustworthiness of a crowdsourcing system. Therefore, the privacy concerns of citizens making use of a crowdsourcing system can be alleviated by increasing the perceived trustworthiness and the information security of the system.

Keywords

Smart city; trustworthiness; information security; privacy

1. Introduction

More than half of the world's population is now living in cities, with this trend towards urbanisation expected to continue in the future (Balta-Ozkan, Davidson, Bicket, & Whitmarsh, 2013). It is thus incumbent on local government to provide public services for this increasing population; however, city infrastructure and resources often have not increased in line with the growing population. This suggests that local governments must find alternative ways of using existing resources more efficiently and effectively (Fuzile, 2011; Harrison & Donnelly, 2011). In order to accomplish these goals and address some of the problems of urbanisation, cities have to become 'smarter' (Karadağ, 2013; Buhl & Jetter, 2009).

Smart cities make use of information and communication technologies (ICT) in order to integrate and connect city services so that the services provided are sustainable and ultimately improve the citizens' quality of life (Dimitriou, 2012). There are a variety of areas in the city that can be improved by making use of the smart city concept. These include the economy, energy, e-governance, mobility, environment and the quality of citizens' lives (Chourabi, et al., 2012).

Smart cities depend on large amounts of information being collected from either the city infrastructure or the citizens in order to be able to make intelligent decisions about city management. The data that is collected can then be analysed in order to anticipate problems or isolate trouble spots (Introna, 1997). There are two types of crowdsourcing method that can be used to collect data from citizens. The first is opportunistic data gathering which takes place when citizens provide information making use of sensors connected to their mobile phones. This type of data gathering is involuntary and the participant does not have control over what data is collected, the time frame for collecting the data, or the location where data will be collected. This data collection method raises serious privacy concerns for citizens who often decline of participate in opportunistic data gathering smart city campaigns (Christin, Kanhere, Reinhardt, & Hollick, 2011; Mehta, 2011).

By contrast, participatory crowdsourcing is a voluntary data gathering method where individuals can choose what they want to report. This approach is particularly useful for unusual events such as accidents or other public safety related problems because citizens can report what they observe in their immediate environment (Halder, 2014). As the person involved can choose what data is reported to a participatory crowdsourcing system, privacy concerns are minimal. However, once the person has reported the information to the crowdsourcing system, they have no control over what is done with it (Bhaveer & Flowerday, 2013). Therefore, information security controls must be in place to ensure that the information reported to the crowdsourcing system remains confidential, maintains integrity and is available to the correct stakeholders (Whitman & Mattord, 2009). Wang, Huang and Louis (2012) report that there is often no transparency concerning the information security controls in crowdsourcing systems, meaning that citizens have no idea whether their data is properly secured. These concerns affect the perceived trustworthiness of the crowdsourcing system and the citizens' participation rate. However, since trust is a subjective term, it is difficult to manage it effectively (Sarwar & Khan, 2013). Consequently, this paper sets out to investigate what the major privacy, information security and trust issues are in current smart cities and how the relationship between these factors influences the decisions of citizens to participate in smart city projects.

The paper is structured as follows: The next section provides a discussion about the privacy concerns of citizens when reporting data to a crowdsourcing system. Then, the concept of information security is discussed with particular reference to the trustworthiness of a crowdsourcing system, after which a brief overview is provided of the methodology used in this study. Next, the results of the study are discussed as they relate to increased citizen participation in a smart city.

2. Privacy

Privacy has been identified as one of the most important considerations for citizens in deciding whether they are willing to participate in smart city initiatives (Pew

Research Centre, 2014). Citizens are becoming more concerned about their privacy as the ability of local government to collect information about them increases. The data that is collected from a citizen can be used to record and track the individual's activities and, coupled with other personally identifiable information, can be viewed as an intrusion of user privacy. As a result, citizens may refrain from participating in smart city projects in order to avert the Big Brother effect (Halder, 2014; Dimitriou, 2012; Chourabi et al., 2012; Christin et al., 2011).

The definition of information privacy that is most relevant to a smart city is that of Westin (1967, p. 1): "Information privacy relates to the person's right to determine when, how and to what extent information about him or her is communicated to others." There are three different concerns when one considers privacy in a smart city. These concerns include the right of the citizen to be left alone, the right of the citizen to control the information collected about them and how the information is used, disclosed to third parties or retained, and the right to be aware what harm may be caused if personally identifiable information is made available to unauthorised parties (Sarwar & Khan, 2013).

Cilliers and Flowerday (2014) reported that the majority of citizens expected detrimental consequences if the information reported to the crowdsourcing system were to be made available to unauthorised parties and they therefore chose to remain anonymous when reporting information to the system. There are four possible consequences for the individual if the information reported to a crowdsourcing system were to be used for malicious purposes (Chourabi et al., 2012). These include intrusion upon one's private affairs; public disclosure of embarrassing private facts about the individual; defamation of character arising from having "private facts" misrepresented in public; and identity appropriation or theft for personal gain by others (Westin, 1967). Therefore, the decision to participate in smart city projects will be determined by the level of privacy and information security that the crowdsourcing system affords citizens (Pew Research Centre, 2014). The next section will discuss the information security necessary in a smart city.

3. Information Security

Information security makes use of proactive measures in order to manage the risks, threats and vulnerabilities related to private information (Parakkattu & Kunnathur, 2010). These measures can protect the privacy of citizens and the information provided to the crowdsourcing system, as they make provision for access controls, retention and storage of information, as well as incident response and recovery procedures (Pearson, 2012).

Whitman and Mattord (2009) report that the most commonly used framework in information security is called the 'C-I-A triad', which refers to the confidentiality, integrity and availability of the information reported to the crowdsourcing system. Confidentiality entails the prevention of any unauthorised disclosure of information reported to the crowdsourcing system, while integrity refers to the protection of the reported information from unauthorised amendment or deletion. The availability of the information is concerned with the ability of all who are authorised to access the information to do so reliably and without undue delay (Suna, Chang, Suna, & Wanga, 2011; Whitman & Mattord, 2009).

Most of the information security problems reported by citizens in a participatory crowdsourcing project can be divided into two categories. The first category considers hardware risks and includes the device that is used to report information to the crowdsourcing system. Mobile devices can be stolen and are vulnerable to security breaches, as the devices lack the computational capacity of personal computers (Wang et al., 2012). Furthermore, once the information is reported, the citizen has to trust that it will be stored securely. The second category has to do with the information that is reported to the crowdsourcing system. Sarwar and Khan (2013) state that the citizen has no control over the ownership of the information once it is reported to the crowdsourcing system; this means that the information can be stolen, used for a different purpose than that originally agreed on, or made available to unauthorised parties. There is also a lack of transparency about the physical location of storage, the security profiles of the site, ownership of the information and what can be done with it (Pearson, 2012). The next section will elaborate on the concept of trust and information security in crowdsourcing systems.

4. Trust

Trust is considered to be a complex social phenomenon (Huang & Nicol, 2014). While there is no universally accepted scholarly definition, trust is understood as a psychological state where an individual has the intention to accept vulnerability or risk based on the positive expectation of the intention or behaviour of another (Pearson, 2012).

There are three characteristics that will determine the perceived trustworthiness of a crowdsourcing system. These are the ability, the benevolence and the integrity of the system (Mayer, Davis, & Schoorman, 1995). The first characteristic, ability, indicates the competency of the crowdsourcing system in performing the expected functions efficiently and consistently (Mallalieu, 2005). In a crowdsourcing system, the ability of the system to record the information reported by the participants correctly will influence this characteristic (Cilliers & Flowerday, 2014). The second characteristic, benevolence, is defined as the extent to which the trustee, that is, local government, is believed to want to act in the trustors', or citizens', best interests. In this study, benevolence refers to the intention of local government to use the information reported to the crowdsourcing system in the best interests of the citizens (Mayer et al., 1995). The last characteristic, integrity, is defined as the perception that, in order to be useful, the information that is reported in a crowdsourcing system must be complete, accurate and current (Cilliers & Flowerday, 2014).

Furthermore, trust can be divided into two categories that will determine the level of perceived trustworthiness of the crowdsourcing system. The first considers preventative security measures that are put in place from a technical point of view (Varadharajan, 2009). These 'hard trust' mechanisms are used to determine the crowdsourcing system's security measures, making use of authenticity controls, encryption, algorithms and audits (Pearson, 2012). Hard trust is often fairly static and the trustworthiness of a system is perceived solely on the basis of the evidence provided by these security measures (Varadharajan, 2009).

The second type of trust is called 'soft trust' and takes into consideration human emotion, perception and experience (Varadharajan, 2009). Unlike hard trust, soft trust is not based on evidence of security credentials, but depends on past interaction with the crowdsourcing system and the recommendations of fellow citizens. Soft security attributes such as the reliability, dependability, benevolence and perceived competence of the crowdsourcing system will all determine how trustworthy the citizens perceive the system to be (Suna et al., 2011). While no crowdsourcing system can be made 100% secure with hard trust mechanisms, soft trust can be used to complement these mechanisms to improve the trustworthiness of the crowdsourcing system (Ling & Masao, 2011).

Information security controls, or hard trust mechanisms, are put in place to protect the information the citizen reports to the crowdsourcing system (Flowerday & Von Solms, 2006). However, the level of trustworthiness will be affected by the perception of how adequate the citizens perceive the security controls that are in place to protect this information to be (soft trust) (Pearson, 2012).

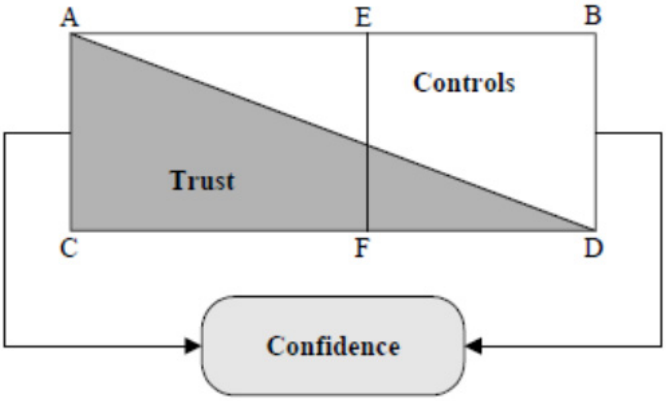

Figure 1: The relationship between trust and controls in a crowdsourcing system (Flowerday & Von Solms, 2006)

Figure 1 illustrates how trust and information security can work together to influence a citizen's decision to participate in a crowdsourcing project. The rectangular area, A, B, D, C, represents the interaction between the citizen and the participatory crowdsourcing system, while triangle A, B, D represents the controls that are inherent to the crowdsourcing system (hard trust). Triangle A, D, C represents the trust that the citizen has that the system will protect their privacy (soft trust). The line E–F is the hypothetical positioning of the citizen's risk appetite, the position of which can be influenced by the individual's propensity to accept risk. When considering the risk appetite line it is clear that the white area is protected by the information security controls and the dark area, which presents risk, is influenced by the perceived trustworthiness of the crowdsourcing system. This means that a citizen's confidence in the crowdsourcing system can be influenced by both trust and information security controls. However, the extent of this confidence will depend on the risk appetite line of the individual (Ling & Masao, 2011).

5. Research Methodology

A positivistic, quantitative study design was used in this project. The study population consisted of citizens living in East London, South Africa. The current East London population is estimated to be 440 000 people (StatsSA, 2011). The general socioeconomic conditions are considered to be poor with the unemployment rate at 28%; in addition, 57% of the population is reported to be living below the poverty line (Managa, 2012).

The University of Fort Hare, in conjunction with IBM, developed an Interactive Voice Response (IVR) system and mobi site which allowed members of the public to report public safety concerns in their immediate environment. The reported data was used in predictive analysis in order to identify problem areas in East London where, if deployed, the limited public safety resources would have the biggest impact.

An IVR system is suitable for developing countries because the existing telephone infrastructure can be used, citizens unfamiliar with the technology can report public safety matters at their own pace, and the IVR system would not exclude illiterate citizens from the project (Whitman & Mattord, 2009). Owing to the high cost of telephone calls in South Africa, the mobi site was introduced as a suitable alternative to the IVR system. During the survey that followed the introduction of the IVR system, citizens indicated no preference for either the mobi site or IVR system when reporting public safety matters. Residents were recruited to participate in this project through marketing in the local newspapers, social media and the distribution of flyers. Figure 2 provides a graphical representation of the project.

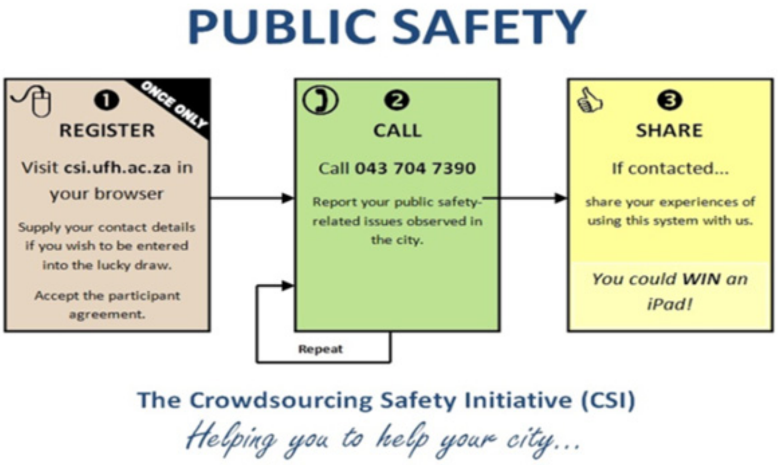
PUBLIC SAFETY
❶ REGISTER
ONCE ONLY
Visit csi.ufh.ac.za in your browser
Supply your contact details if you wish to be entered into the lucky draw.
Accept the participant agreement.
❷ CALL
Call 043 704 7390
Report your public safety-related issues observed in the city.
Repeat
❸ SHARE
If contacted...
share your experiences of using this system with us.
You could WIN an iPad!
The Crowdsourcing Safety Initiative (CSI)
Helping you to help your city...

Figure 2: Steps in the crowdsourcing system

A total of 485 people registered for the project and were subsequently sent a questionnaire to complete at the end of it. The questionnaire was compiled making use of previously published material in the area of information security and trust. Information security was tested making use of 3 variables: Availability, Confidentiality and Integrity of the crowdsourcing system while the trustworthiness of the system was tested making use of 3 variables: Benevolence, Integrity and Ability of the system to accurately reflect the public safety concerns of the citizens of East London (Refer Table 1 for questions). A total of 361 questionnaires were completed and returned. Thus, the response rate was 81.2%. The Cronbach's alpha coefficient was computed and was found to be 0.9, which is considered to indicate good test reliability. Ethical approval for the study was obtained from the Research Ethics Committee of the University of Fort Hare.

6. Results and Discussion

This paper discussed the relationship between privacy, information security and the perceived trustworthiness of a crowdsourcing system in a smart city. The study sample consisted of 219 (60.7%) males and 142 (39.3%) females. Seventy-one per cent of the participants were younger than 40 years of age. The 40 to 49 year age group consisted of 14.7% of the study sample, while the two oldest age groups, 50 to 59 and 60+ were the smallest groups with percentages of 10.2 and 3.3%, respectively.

Correlation analysis tests were conducted to determine whether relationships existed between the different factors identified for these two constructs in the literature section. The correlation coefficients provide an indication of whether the relationship is a positive relationship (changes to constructs increase or decrease in the same direction) or a negative relationship (constructs respond in opposite directions). The results for the information security factors (confidentiality, integrity and availability) and the trust factors (integrity, benevolence and ability) are displayed below.

As shown in Table 1, Pearson's correlation coefficient was used to investigate the relationship between the factors contributing to information security and the trustworthiness of the crowdsourcing system. A p-value of less than 0.001 was chosen to indicate statistical significance.

The relationships between the information security and the trustworthiness of the crowdsourcing system were found to be statistically significant, as positive correlations are shown with a p-value smaller than 0.001. These findings illustrate that it can be anticipated that information security will increase the perceived trustworthiness of a crowdsourcing system among citizens, which in turn will increase participation in smart city projects.

			Confidentiality	Integrity	Availability
			I prefer to provide information anonymously	I do not worry that the information I provided will be modified in any way	The IVR system must be available 100% of the time in order to be useful
Integrity	The information that is reported in a participatory crowdsourcing system must be complete, accurate and current in order to be useful	Pearson Correlation	164.573	97.067	375.730
		Sig. (2-tailed)	0.00	0.00	0.00
		N	361	361	361
Benevolence	I do not worry if the information provided will be used for something other than the intended purpose	Pearson Correlation	98.509	205.753	66.704
		Sig. (2-tailed)	0.00	0.00	0.00
		N	361	361	361
Ability	I trust the system to reflect my public safety matter correctly	Pearson Correlation	183.632	70.912	393.119
		Sig. (2-tailed)	0.00	0.00	0.00
		N	361	361	361

Table 1: Correlation between information security and trust factors

From the statistical tests conducted in this section, it is clear that there is a direct correlation between the trustworthiness of a crowdsourcing system and information security in place to protect the privacy of the citizens. The information security controls in a crowdsourcing system are not always transparent, meaning that the majority of the citizens (72.6%) preferred to remain anonymous when reporting information to the system (confidentiality). The citizens also agreed that for the system to be useful, it must be available all the time (86.6%). The integrity of the system was more of a concern for citizens, however, as more than a third (37.5%) raised concerns that the information could be modified in some way.

The citizens did believe that the crowdsourcing system would be able to reflect their public safety concerns correctly (84.0%), while 86.6% agreed that the information reported must be complete and accurate in order to be useful. This is especially important in the public safety context as the information will be used to determine the correct response to emergency situations. The citizens were concerned about the intended purpose of the information reported, with 42.2% reporting that they were concerned that the information may be used inappropriately.

7. Conclusion

In view of the resource constraints experienced by local authorities in developing countries, they must find ways to make use of existing resources more effectively and efficiently. Accordingly, smart cities make use of ICT to collect data that can be analysed to predict where resources will be needed or will have the biggest impact. In view of the fact that large amounts of data have to be collected, citizens participating in these projects have certain privacy concerns. One of the ways in which to address these privacy concerns, and subsequently increase the participation of citizens in smart city projects, is to enhance the perceived trustworthiness of the crowdsourcing making use of information security controls. This study found that there is a positive relationship between the privacy concerns and perceived trustworthiness of the crowdsourcing system. The trustworthiness of a crowdsourcing system can be increased by implementing appropriate information security controls. Consequently, further research in the field needs to investigate the specific influence that either soft and hard trust mechanisms have on the perceived trustworthiness of the crowdsourcing system. Appropriate feedback mechanisms should also be investigated to find the most appropriate mechanism for the public safety context.

8. References

ACOPEA. (2012). African Child Online Protection Education \& Awareness Centre. available online from: http://www.cto.int/media/events/pst-ev/2013/CTO%20Forum/African%20Child%20Online%20Protection%20Education%20\&%20Awareness%20Centre.pdf, Accessed on [12 November 2013].

Antwi-bekoe, E., & Nimako, S. G. (2012). Computer Security Awareness and Vulnerabilities : An Exploratory Study for Two Public Higher Institutions in Ghana. Journal of Science and Technology , 1, 358-375.

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people . Computer Fraud \& Security , 2009 (7), 13-19.

Ayodele, T., Shoniregun, C., & Akmayeva, G. (2012). Anti-Phishing Prevention Measure for Email Systems. Internet Security (WorldCIS), (pp. 208-211). Guelph.

Balta-Ozkan, N., Davidson, R., Bicket , M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. Energy Policy, 63 , 363-374.

Becta. (2009). AUPs in context: Establishing safe and responsible online behaviours. available online from: http://education.qld.gov.au/studentservices/behaviour/qsaav/docs/establishing-safe-responsible-online-behaviours.pdf, Accessed on [10 November 2013].

Bhaveer, B., & Flowerday, S. (2013). Using participatory crowdsourcing in South Africa to create a safer living environment. International Journal of Distriuted Sensor Networks , 1-13.

Buhl, H. U., & Jetter, M. (2009). BISE's Responsibility for our Planet. Business and Information Systems Engineering, 1(4) , pp. 273-276.

Byron, T. (2008). Safer Children in a Digital World. available online from: http://webarchive.nationalarchives.gov.uk/20130401151715/https://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf, Accessed on [5 November 2013].

Caragliu, A., Del Bo, C., & Nijkamp, P. (2009). Smart Cities in Europe. Series Research Memoranda 0048. Amsterdam: University of Amsterdam, Faculty of Economics, Business Administration and Econometrics.

Chen, J., & Guo, C. (2006). Online Detection and Prevention of Phishing Attacks. Communications and Networking in China, 2006. ChinaCom '06. First International Conference, (pp. 1-7). Beijing.

Chourabi, H., Nam, T., Walker , S., Gil-Garcia, J., Mellouli, S., Nahon, K., et al. (2012). Understanding Smart Cities: An Integrative Framework. 45th System Science (HICSS) Hawaii International Conference (pp. 2289-2297). Hawaii: HICSS.

Christin, D. (2010). Impenetrable Obscurity vs Informed Decisions: Privacy Solutions for Participatory Sensing. In Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications (pp. 847-848). Mannheim: IEEE.

Christin, D., Kanhere, S., Reinhardt, A., & Hollick , M. (2011). A Survey on Privacy in Mobile Participatory Sensing Applications. Journal of Systems and Software, 84(11) , 1928-1946.

Cilliers, L., & Flowerday , S. (2014). Information security in a public safety, participatory crowdsourcing smart city project. World CIS Conference (pp. 1-5). London: World CIS.

Cole, K., Chetty, M., Larosa, C., Rietta, F., Schmitt, D. K., & Goodman, S. E. (2008). Cybersecurity in Africa : An Assessment. available online from: http://s3.amazonaws.com/zanran_storage/www.cistp.gatech.edu/ContentPages/43945844.pdf, Accessed on [22 November 2013].

de Lange, M., & von Solms, R. (2012). An e-Safety Educational Framework in South Africa. Proceesing of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC) .

Dimitriou, T. (2012). Smart Internet of things in future cities (with emphasis on security). Berlin: Germany.

Dlamini, I., Taute, B., & Radebe, J. (2011). Framework for an African policy towards creating cyber security awareness. Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW) , 15-31.

e4Africa. (2011). Technology in schools – for better or for worse. available online from: http://www.e4africa.co.za/?p=3516, Accessed on [20 November 2013].

Flowerday, S., & Vol Solms, R. (2006). Trust: An Element of Information Security. SEC .

Furnell, S. (2005). Why users cannot use security. Computers & Security (24), 274-279.

Fuzile, L. (2011). Local Government budgets and expenditure. Pretoria: National Treasury.

Grobler, M., & Dlamini, Z. (2012). Global Cyber Trends a South African Reality. IST-Africa 2012 Conference Proceedings .

Halder, B. (2014). Evolution of crowdsourcing: potential data protection, privacy and security concerns under the new Media Age. Democracia Digital eGoverno Electronico , 337-393.

Harrison, C., & Donnelly, I. (2011). A theoryof smart cities. Proceedings of the 55th Annual Meeting of the ISSS. London: University of Hull Business School.

Huang, J., & Nicol, D. (2014). Evidence-based trust reasoning. HotSoS2014 (pp. 1-2). Raleigh: ACM.

IBM. (2010). Smarter Thinking for a Smarter Planet. Retrieved February 28, 2013 from IBM: http://www.ibm.com/smarterplanet/global/files/us_en_us_1oud_ibmlbn0041_transtasman_book.pdf

Introna, L. (1997). Privacy and the computer: why we need privacy in the Information Society. Metaphilosophy, 28(3) , 259-275.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2005, December 15). Social Phishing. Bloomington.

Janssen, C. (n.d.). Spear Phishing. Retrieved April 29, 2013 from Techopedia: http://www.techopedia.com/definition/4121/spear-phishing

Jisc. (2012). A guide to open educational resources. available online from: http://www.jisc.ac.uk/publications/programmerelated/2013/Openeducationalresources.aspx Accessed on [20 November 2013].

Kanyesigye, F. (n.d.). New drive to fight hackers, New Times. available online from: http://www.newtimes.co.rw/news/index.php?a=66437&i=15343, Accessed on [22 November 2013]. , 2013.

Karadağ, T. (2013). An evolution of the Smart City Approach. Middle East Technical University.

Kortjan, N., & von Solms, R. (2013). Cyber Security Education in Developing Countries: A South African Perspective. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering , 119, 289-297.

Kritzinger, E. (2011). Cyber Awareness Implementation Plan (CAIP) for schools. Presentation for Southern African Cyber Security Awareness Workshop (SACSAW) .

Ling, A., & Masao, M. (2011). Smart grid information security (IS) functional requirements. arXiv preprint arXiv:1109.4474, 2011.

Mallalieu, L. (2005). An examination of the role of customer attributions in understanding trust loss and recovery in buyer-seller relationships. Supply Chain Forum: an International Journal, 6(2) , 68-80.

Managa, S. (2012). Unfulfilled Promises and their Consequences: A Reflection on Local Goverment Performance and the Critical Issue of Poor Service Delivery in South Africa . Africa Insitute of South Africa , 76, 1-8.

Mars, M., & Erasmus, L. (2012). Telemedicine can lower health care costs in Africa. Innovate , 7, 32-33.

Mayer, R., Davis, J., & Schoorman, F. (1995). An integrative model of organizational trust. Academy of Management Review , 20 (3), pp. 709-734.

Mehta, S. M. (2011, August 25). Mobile 311: a framework for 311 services with mobile technology. San Diego: San Diego State University.

Migrant. (2013). M-PESA International Money Transfer Service, Safaricom. available online from: http://www.ilo.org/dyn/migpractice/migmain.showPractice?p_lang=en\&p_practice_id=70, Accessed on [12 November 2013].

Miles, D. (2011). Youth protection: Digital citizenship - Principles and new resources. Second Worldwide Cybersecurity Summit (WCS), (pp. 1-3).

OER_Africa. (2013). Understanding OER. available online from: http://www.oerafrica.org/understandingoer/UnderstandingOER/tabid/56/Default.aspx, Accessed on [20 November 2013].

Parakkattu, S., & Kunnathur, A. (2010). A framework for research in infomration security management. Northeast Decision Sciences Institute Proceedings , 318-323.

Pearson, S. (2012). Privacy, security and trust in cloud computing. New York: IBM.

Pew Research Centre. (2014). Emerging nations embrace the Internet. Washington: Mobile Technology.

PWC. (2012). Telecoms in Africa: innovating and inspiring. Communications Review .

Reed, M. (2012). Press release: Africa mobile subscriptions count to cross 750 million mark in fourth quarter of 2012. Informa Telecoms \& Media .

Safaricom. (2012). iCow. available online from: http://www.safaricom.co.ke/personal/value-added-services/social-innovation/icow, Accessed on [12 November 2013].

Safaricom. (2012). Relax, you've got M-Pesa. available online from: http://www.safaricom.co.ke/personal/m-pesa/m-pesa-services-tariffs/relax-you-have-got-m-pesa, Accessed on [12 November 2013].

Sarwar, A., & Khan, M. (2013). A review of trust aspects in cloud computing security. International Journal of Cloud Computing and Services Science , 116-122.

Sato, N. (2013). ICT stakeholders discuss emerging issues on African cyber security. available online from: http://www.humanipo.com/news/32773/ict-stakeholders-discuss-emerging-issues-on-cyber-security, Accessed on [21 November 2013].

Spamhaus. (2010, January). Whitepapers: Effective filtering. Retrieved July 16, 2013 from Spamhaus: http://www.spamhaus.org/whitepapers/effective_filtering/

StatsSA. (2011). Key results: Census 2011. Retrieved January 21, 2015 from Stats South Africa: www.statssa.gov.za/Census2011/.../Census_2011_Key_results.pdf

Suna, D., Chang, G., Suna, L., & Wanga, X. (2011). Advanced in Control Engineering and Information Science surveying and analysing security, privacy and trust issues in cloud computing environments. Procedia Engineering , 2852-2856.

TeleGeography. (2013). Africa’s international bandwidth growth to lead the world. TeleGeography: Global Bandwidth Forecast Service .

Think_U_Know. (2008). Welcome to Hector's World. available online from: http://www.thinkuknow.co.uk/5_7/hectorsworld/, Accessed on [15 November 2013].

Varadharajan, V. (2009). A note on trust-enhanced security. IEEE Security and Privacy, 7 , 57-59.

Wang, Y., Huang, Y., & Louis, C. (2012). Respecting user privacy in mobile crowdsourcing. ASE2012 (pp. 1-15). London: ASE.

Westin, A. (1967). Privacy and Freedom. New York: Atheneum Publishers.

Whitman, B., & Mattord, H. (2009). Principles of information security. Boston : Thomson Course Technology.