ISBN: 978-989-8704-02-3 © 2014 IADIS

LEARNER CENTRIC IN M-LEARNING: INTEGRATION OF SECURITY, DEPENDABILITY AND TRUST

Sheila Mahalingam, Faizal Mohd Abdollah and Shahrin Sahib
C-ACT Faculty of Information Technology and Communication, Univeristi Teknikal Malaysia Melaka,
Locked Bag 1752, Pejabat Pos Durian Tunggal, Melaka, 76109 Malaysia

ABSTRACT

The paper focus on learner centric attributes in a m - learning environment encounters the security measurements. In order to build up a systematic threat and countermeasure for protecting the learners as well as providing awareness and satisfaction in utilizing the mobile learning system, a security model need to be overhauled. The brief literature survey is conducted and analyst to produce a new classification and definition. The paper introduces new definition, concepts and classification model integrating security and dependability for a learner centric security model and evaluation to assess the confidence and satisfaction level of learners.

KEYWORDS

Leaner Centric, Security, Dependability, Trust, Satisfaction.

1. INTRODUCTION

In today's emerging mobile world that are widely accepted by people in the use of many kinds of applications, presence of vulnerabilities, threats, faults, failure and error is unavoidable and the information technology application, devices and models will never be entirely secure. Security dependability and trust need a mechanism for the changing and evolving environment issues and should be able to resist future unpredictable threats (Savola 2009).Without adequate protection towards the devices, networks and applications, services and personal data, trust will slowly vanish out from the user perception in mobile systems.(Basili et al. 2004) mentioned that The International Federation for Information Processing Working Group 10.4 defines dependability as trustworthiness of a computing system which allows confidence and trust to be justifiably placed on the service delivers. Security will have to be ensured from end to end point which is from application layer right up to the physical layer. Traditionally there are two different communities separately working on the issues of dependability and security. One is the community of dependability that is more concerned with non malicious faults(Buja & R.Menis 2006; Avizienis et al. 2001; Birolini 2004; Laprie & Roche 1995; JC Laprie 1992), to name one of just a few. The other is the security community that is more concerned with malicious attacks or faults (Molisz 2004; Medhi & Tipper 2000).

Integrating the security and dependability in a trusted environment introduces a new classification in security, especially a new platform to mobile learning scheme and mobile learners. It gives a reliable platform to user to adopt m-learning in a secure environment and introduces awareness to the learners as well as help the higher learning strategic plan team to understand the security constraints involved in implementing m-learning in the future.

2. THEORITICAL JUSTIFICATION AND RELATED WORKS

Dependability was first introduced as a generic term encompassing concept such as reliability, availability, maintainability and safety as well as related measures. (A, Laprie, B, & C, 2004; Avizienis et al., 2001; Buja & R.Menis, 2006; Laprie & Roche, 1995; J.C.Laprie, 1995; Neogy, 2010;Meadows, 1995; Meadows & McLean, 1999; Zhang, Chuang, & Kong, 2009; Dhama et al., 2009) presented two alternative definitions for dependability as the first one is “the ability to deliver service that can be justifiably trusted” and secondly “ability to avoid service failures that are more frequent and more severe than is acceptable”. A more rigorous definition and classification of dependability can be found from(Jonsson 1998);(Jonsson et al. 1999);(E. Jonsson, 2006a);(Jameel et al. 2005).However (Trivedi et al. 2009)several dependability classification exist but not all are useful to quantitatively access the attributes which some still need qualitative measures and access the attributes of variety of system networks as mentioned is the previous study. (Savola 2009) inputs for mobile devices are still not well defined , incorrect, and cannot be accepted as harmless because mobile devices are still defective and dependability of the system is becoming more and more critical.Security in a traditional definition refers to actions taken to protect data against unauthorized disclosure, alteration and destruction.(Erland Jonsson, 1998;Catherine Meadows, 1995; C. Meadows & McLean, 1999) presented an outline of a fault model for security and showed how it could be applied to both fault tolerance and fault forecasting in computer security. Security researchers consider confidentiality, integrity, and availability and sometimes, non-repudiation or authenticity to represent the security status of the system and networks but it is lack of representing reliability and performance (Trivedi et al. 2009). (JC Laprie 1992) described the extended attributes that are relevant to security such as robustness, accountability, authenticity and non repudiation. There is a huge database of theoretical work that focuses on different security related properties and different type of information security models (R. Savola, 2007; Daniels, 1989; C.Wang, 1997; K. Zhang, 1997; McLean, 1990; McCullough, 1998) and continuous effort to new approaches on security which has started from dependability approach and continued with security techniques. The security of mobile communications has, and will continue to be, a core issue of high practical relevance and therefore an adequate protection to devices, networks, applications, services and personal data are needed because the trust and confidence in mobile systems would quickly vanish, as has been the case with so many Internet-based services (Savola 2009).In the near future (Yang & Peterson 2004) the concept of trust will become more essential since it is a complex concept with many different attributes relies within it such as dependability, truthfulness, security and etc. In the emerging wireless and future mobile technologies and communications they need to differentiate between trust, security and dependability concepts and the relationship is in demand.The trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers (E.Jonsson, 1993;JC Laprie, 1992;Kyriakopoulos et al., 2009;Erland Jonsson et al., 1999).It is suggested as an extension of dependability in (Dobson et al. 1990)by giving judgment on the accepted ability of the system rather than being a property of the system. (Hu et al. 2011)explained that the concept of trustworthiness is appropriate for large and complex systems with ambiguous or inconsistent. According to (Savola 2009), user trust and actual trustworthiness of the mobile solutions need to be balanced since the user population of mobile devices and services is growing, both in the consumer market and in professional use. Furthermore trust should always be obtained, measured and accessed in order to preserve the user’s confidence that she or he can keep the service under control and that the service will not misuse their personal data or information. More rigorous work done by (Jameel et al. 2005)proposed a model for evaluating trust based on vectors of trust beside basic factors of trust computation.

Studies argued for the need of integration of dependability and security and it is important to have a cross discipline task to establish generic, widely and unambiguous trust model (Savola 2009).Brief description of the system model for security and dependability attributes originally proposed in (Erland Jonsson, 1998 ;Erland Jonsson, Strömberg, & Lindskog, 1999 ;E. Jonsson, 2006b)from the standpoint of behavioral and preventive terms. (Avizienis et al. 2001)defined and summarized fundamental concepts of dependability. They presented the pathology of a failure and they compared the definitions of three widely known concepts: dependability, survivability, and trustworthiness. The classical definition of dependability encompasses the attributes of reliability, availability, safety, integrity, and maintainability. The classical definition of a security encompasses the attributes of confidentiality, integrity, non-repudiation, and availability. (Nicol et al. 2004)presented measures of dependability and security and reviewed model representation/analysis techniques. (Sallhammar 2007)proposed an approach to integrate security and dependability evaluation based on stochastic models.Other integrative approaches to security and dependability are found in (Laprie & Roche, 1995; Hu et al., 2011; Trivedi et al., 2009; R. Savola, 2007 ;Sallhammar, 2007; Catherine Meadows, 1995; C. Meadows & McLean, 1999; Nicol et al., 2004 (Sun et al. 2010) (Hu et al. 2011) (Serpanos & Henkel 2008) (Spanoudakis 2008) (JC Laprie 1992) (Jameel et al. 2005) (E.Jonsson 1993) Erland Jonsson & Laleh Pirzadeh, 2011) as well as in the results of MAFTIA project (Project IST Research 2003)and SecurIST project (Project IST Research 2003).

3. NEW DEFINITION, CONCEPT AND CLASSIFICATION

At the user level point of view availability is therefore best regarded as a separate attribute reflecting whether or not the system can deliver its services. At the same time to possibly accept a low reliable system that must be available as system failures can be remedied quickly and does not involve the delivery time However on this model availability is chosen to be the appropriate methods at user level because reliability ensures availability and if the system is reliable that means the system is able to detect repair or tolerant fault and run in a secured and secure state. Reliability will be the transparent attribute of availability; reliability works at the system level and availability works at the user level. This availability attributes represents the learners and non learners behavioral attributes of dependability. ***Dependability Behavioral Attribute (Availability)**: The ability of the system to be connected easily and links are available at a minimum pre specified level of usage with system remain operable and maintain performance in the event of one or more specified threat.*

Accessibility is generalized under the hierarchy if information system which gives an importance to the user's experience. This could be much related to the m-learning environment as learners from various locations with a variety of devices need to access to the system without failure. To extend these concern accessibility is strongly related to user level terminology of m learning system. Furthermore accessibility attributes is used in this model because in (Zeta Dooly, Jim Clarke, W. Fitzgerald, W. Donnelly, WIT; Michel Riguidel, ENST; Keith Howker 2007) project reports a mechanism and tool are needed for accessing and proving the level of security and dependability of ubiquitous environment which substitutable to m-learning system. The security level applied to the mobile will impact the accessibility of the systems. ***Security Protective Attribute (Accessibility):** Ensure the mobile learning system and data are highly accessible at all times, preventing denial of service attacks with maintaining authenticity to authorized learners and disclosure data and system in trust environment***.**

Users need to know that service is existence, know the ways they can contact and access the services (EL-Kiki & Lawrence, 2006). On the user perspective quality of a service is much closer related to awareness which refers to degree of goodness and usefulness of the services given by the system. Mobile learners need to get convenience, expediency and immediacy of mobile learning in appropriate time and accessing the appropriate learning contents (K.S, Daniel Su, 2006). Address here that if a learner are aware of usability of the mobile system, it means the extent to which m-learning system can be used by the specified users to achieve their learning goal with efficiency, satisfaction and acceptance to use the content of the system. Awareness guidelines empower the effort in creating highly acceptable and trust to use the system which promotes learners satisfaction while learning via mobile and ensemble devices. ***Security Behavioral Attribute (Awareness):** Knowledge and attitude of learners in m-learning system regarding the protection of ensemble mobile devices with secure behavior by understanding potential threats.*

As suggested here is a learners' environment integrated with security and dependability interrelates with trust, as dependability is a subjective and reflects the learners's degree of trust towards the m-learning system. The learner's environment illustrates the interaction between learners and well established, trusted system domain knowledge. *Mobile Learners are classified into a secure domain holding the attribute of awareness, accessibility and availability which give a complete trust towards using the m-learning system via their ensemble mobile device.* Therefore, it is clearly stated that personalization in a mobile learning environment to be introduced representing qualitative judgment of learners security assessment via factors that involved with user or learners direct contact to trust. This study considers availability, accessibility and awareness as security attributes for mobile learners in mobile learning. Precedent studies showed that the trust played an important role in the security, satisfaction of learners in mobile learning acceptance as a formal learning tool. The Learner Centric Security Model developed in this study integrates theories of security and dependability. Briefly the model composed of three aspects; (i) Learner & Device (ii) Security & Dependability and (iii) Trust & Satisfaction. These three aspects combine to develop a description of m-learning at user level. The criteria for the evaluation instruments were based upon this description. Figure 1 illustrates the new classification of dependability and security integration at learners level trustworthy

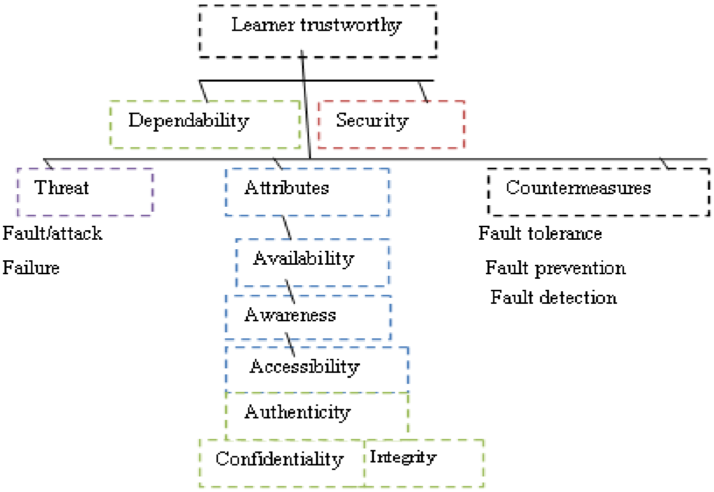

Figure 1. A new classification of dependability and security at learners level trustworthy

4. DISCUSSION AND FUTURE EFFORTS

The research study compromises the overall understanding of new security and dependability integration in mobile learning specifically at learner centric environment.The proposed model was tested emprically using data collection from survey investigating security awareness containing constructs in the model.The study presents an extended technology acceptance model(TAM) evaluation to explore the factors and hyphotheses that affects satisfaction to use mobile learning.The overall model will be validated through mix method of focus group case study and panel expert interviews. The results from the study can be used as additional information when improving or integrating learners' mobile security in mobile learning system and contributes to the body of knowledge of mobile learning security awareness by addressing the identified gaps.

ACKNOWLEDGEMENT

The author wishes to thank the University of Technical Malaysia, Melaka (UTEM), Centre for Graduate Studies (CGS) and Faculty of Information Technology and Communication (FTMK). This work was supported in part by a scholarship from the Department of Public Service Malaysia (JPA) and Ministry of Higher Education Malaysia (MOHE).

REFERENCES

A, A. et al., 2004. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1), pp.11–33.

Avizienis, A., Laprie, J.-C. & Randell, B., 2001. *Fundamental concepts of dependability*,

Buja, G. & R.Menis, 2006. Conceptual Frameworks for Dependability and Safety of a System. In *International Symposium on Power, Electronics, Electrical Drives, Automation and Motion,SPEEDAM 2006,*. Taormina (Sicily)-ITALY, pp. 44–49.

Daniels, B.K., 1989. Department of Defense,Trusted Computer System Evaluation Criteria("orange book") CSC-STD-001-83. In T.Anderson, ed. *"Errors, faults and failures: A model", in Safe and Secure Computing Systems*. Blackwell Scientific Publications, p. 256. Available at: http://www.fishpond.com.my/Books/Safe-and-Secure-Computer-Systems-TA-Anderson-Edited-by/9780632018192.

Dobson, J., McDermid, J. & Randell, B., 1990. *“On the Trustworthiness of Computer Systems” ESPRIT/BRA Project 3092 Technical Report Series No. 14, 1990*,

Hu, J. et al., 2011. Journal of Network and Computer Applications Seamless integration of dependability and security concepts in SOA : A feedback control system based framework and taxonomy $. *Journal of Network and Computer Applications*, 34, pp.1150–1159.

Jameel, H. et al., 2005. A Trust Model for Ubiquitous Systems based on Vectors of Trust Values. In *Seventh IEEE International Symposium on Multimedia*.

JC Laprie, 1992. *Dependability: Basic Concepts and Terminology,* J.C Laprie., Spring-Verlag. Available at: iet.unipi.it.

Jonsson, E., 2006a. Towards an integrated conceptual model of security and dependability. *First International Conference on Availability, Reliability and Security (ARES’06)*, p.8 pp.–653. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1625369.

Kyriakopoulos, N., Member, S. & Hussein, S., 2009. A Comparative Analysis of Network Dependability, Fault-tolerance, Reliability, Security, and Survivability. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,*, 11(2), pp.106–124.

Laprie, J. & Roche, C., 1995. Dependable Computing : Concepts , Limits , Challenges. In *FTCS-25, The 25th IEEE International Symposium on Fault-Tolerant Computing*. Pasedena , California , USA: IEEE, pp. 42–54.

McLean, J., 1990. Security models and information flow. In *Proceedings. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, 7-9 May 1990*. Ieee, pp. 180–187. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=63849.

Meadows, C., 1995. Applying the Dependability Paradigm to Computer Security. In *Proceedings of 1995 New Security Paradigms Workshop*. IEEE Computer Society Press, pp. 75–81. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=492346.

Nicol, D.M., Sanders, W.H. & Trivedi, K.S., 2004. Model-Based Evaluation : From Dependability to Security. *IEEE Trans. Dependable and Secure Computing*, 1(1), pp.1–17.

Sallhammar, K., 2007. *Stochastic Models for Combined Security and Dependability Evaluation*. Norwegian University of Science and Technology.

Savola, R., 2007. Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry. In *Software Engineering Advances, 2007. ICSEA 2007.* Cap Esteral, France, p. 60. Available at: ieeexplore.ieee.org/iel5/4299876/4299877/04299940.pdf.

Serpanos, D. & Henkel, J., 2008. Dependability and Security Will Change Embedded Computing. *IEEE Computer Society*, (January), pp.103–105.

Spanoudakis, G., 2008. Monitoring Security and Dependability in Mobile P2P Systems. *3rd International Conference for Internet Technology and Secured Transactions (ICITST ’08).*

Trivedi, K.S., Kim, D.S. & Roy, A., 2009. Dependability and Security Models. In *Proceeding of 7th International Workshop on the Design of Reliable Communications Networks DRCN 2009*. Washington DC.

Zeta Dooly, Jim Clarke, W. Fitzgerald, W. Donnelly, WIT; Michel Riguidel, ENST; Keith Howker, V., 2007. *SecurIST D3 . 3 – ICT Security & Dependability Research beyond 2010 : Final strategy*,

Zhang, X., Chuang, L. & Kong, X., 2009. Model-Driven Dependability Analysis of Virtualization Systems. In *Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference*. Shanghai: IEEE Comput. Soc. Press, pp. 199 – 204.