International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:7, No:9, 2013

E-government Security Modeling: Explaining Main Factors and Analysing Existing Models

N. Alharbi

***Abstract*—**E-government is becoming more important these days. However, the adoption of e-government is often slowed down by technical and non-technical security factors. Nowadays, there many security models that can make the e-government services more secure. This paper will explain the main security factors that affected the level of e-government security. Moreover, it will also analyse current existing models. Finally, the paper will suggest a comprehensive security model that will contain most of technical and non-technical factors.

***Keywords*—**E-government, technical, non-technical, security model.

I. Introduction

E-government can be defined as a way to improve the quality of government services and to encourage greater participation in democratic processes, by using innovative ICT technologies [1]. This definition is from technological perspective since there is no general definition for e-government that can cover all areas [2]. There are four main types of e-government as in Fig. 1, which are, Government to Government (G2G), Government to Citizens (G2C), Government to Business (G2B) and Government to Employees (G2E) [3]. One of the main factors that effected the adoption of e-government is the lack of security [4]. Security issues can be divided into two groups. The first group is technical issues such as confidentiality, integrity and availability. The second group is non-technical issue such as trust, lack of awareness, computer literacy and privacy. Security models will be analysed in this paper as well. These models are also based on technical or non-technical issues. There are a lot of researches focusing in e-government security in developed countries and few researches have been done in developing countries [5]. Even though, the effective of non-technical issue have been seen clearly in developing countries [6]–[8]. In addition, most of these models are based on functionality. As a result, there is ashortage of researches that focusing on non-technical issues [5].

II. Main Affected Factors on E-Government Security

This paper will explain most important factors that effected on e-government security wither they are technical or non-technical factors and tables.

N. Alharbi is with Centre for Security, Communications and Network Research, Plymouth University, Plymouth, United Kingdom (e-mail: nawaf.alharbi@plymouth.ac.uk).

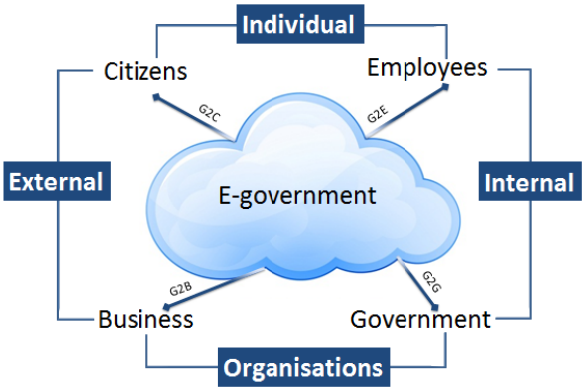

Fig. 1 Types of e-government

A. Confidentiality

It means that only authorised users can access to the government data. Unauthorised users will be prevented.

B. Integrity

Integrity means that all e-government data will be saved and cannot be changed or modified.

C. Availability

E-government portal and other government services must be available all time and can be accessed easily. The popular attack effect this factor is Denial of Service (DoS).

D. Privacy

It means that both of personal data and government websites must be free from being observed by other people. Users will not use e-government services if the privacy is not guaranteed [9].

E. Lack of Awareness

It has been observed that lack of awareness affected the security level of e-government services especially in developing countries [10].

F. Trust

There are two parts in trust can be affected. First, Trust Of the Internet (TOI). Users need to trust using internet and be confident of passing their information on the internet. Second, Trust Of Government (TOG). Sara indicates that “In many developing countries, citizens do not trust their governments, especially when there has been a history of dictatorship, political instability or large-scale corruption” [11].

G. Computer Literacy

Computer literacy plays an important role in e-government security. People with low knowledge of using computer will not be able to use e-government services safely.

III. Existing Security Models and Theories

This paper divided the models and theories that are using on e-government security to technical and non-technical groups. There is no model covers both of technical and non-technical issues in the same time [1].

A. Technical Models

This paper will analyse the most important security models.

1. Bell-LaPadula (BLP) Model

This model is the first security model and it is focusing on confidentiality. It is one of popular security models. The shortage of this model is that this model does not solve other security issues such as integrity and availability sine it is focusing on confidentiality only. However, this model is still used as a multilevel security model even that it cannot meet the current security requirements these days [12].

2. BibaModel

Biba is the first security model that is focusing on integrity. This model also does not meet the security requirements these days. However, the main feature of this model that it can be integrated with BLP model easily. This model is based on Low Water Mark Principle [12]. Biba model is working opposite of BLP. It is known as "BLP upside down" [13].

3. Clark-Wilson Model

This model is also focusing on integrity as well. It widely use in bank system as integrity in bank system is more important than confidentiality. However, this model is complex and does not solve other security issues [12].

4. The Chinese Wall

The main goal of this model is to protect the system from any conflict between each node in the system. In addition, it provides privacy and integrity as well.

5. LambrinoudakisSecurity Framework

This framework is developed to protect the system from DoS and being effected by malicious. It contains five steps (setting up the supporting system, authentication, setting up the service, offering the service, and after service task).

6. InfosecModel

This model is one of the earliest models in information security. It covers confidentiality, integrity and availability. This model can reduce the vulnerabilities and probability of completed attacks and selecting the best action to protect the system from electronic eavesdropping [13].

B. Non-Technical Models and Theories

Most of non-technical issues came from human behaviour. Thus, many of researches are applied by using acceptance theories.

1. Theory of Reasoned Action (TRA)

This is the first theory that is trying to understand the human behaviour by Ajzen and Fishbein. It is mainly focus on behavioural intention against new technology. The theory is based on four parts, behaviour, behavioural intention, attitude toward behaviour and subjects norm [14].

2. Theory of Planned Behaviour (TPB)

This theory is developed byAjzen and Fishbeinto fill the gaps in TRA theory. It is an extended theory of TRA since it contains the same four parts of TRA with perceived behavioural control (PBC) as an additional part [14].

3. Technology Acceptance Model (TAM)

TAM is another information system model that is focusing on the users' acceptance of new technology and the factors that influence their decision of using this new technology. This model was developed by Davis and Bagozzi. It contains two factors: Perceived usefulness (PU) and Perceived ease-of-use (PEOU) [15].

4. Diffusion of Innovation (DOI)

DOI is a theory by Rogersandit rates the acceptance of new technology though cultures and explaining the reasons of its spread and how this has been done. Rogers sets five elements for his theory. Four of them have a positive effect (Trialability, observability, relative advantage and compatibility) and the one has a negative effect which is complexity [14].

5. Motivational Model (MM)

MM can explain behaviours in different environments and situations which is the main advantage of this model. MM is based on two parts: Frist, intrinsic motivation. Second, extrinsic. This model has been tested by Davis who found that both of these parts are the main factors in intention to perform the behaviour in the context of using the technology [15].

6. Social Cognitive Theory (SCT)

SCT is a learning theory and it explains that people usually follow other people and they do the same thing. There are four factors in this theory, drives, cues, responses and rewards [13].

7. Model of PC Utilization (MPCU)

MPCU has two factors that have not been covered in previous models which are job fit and facilitating conditions [16].

8. Unified Theory of Acceptance and Use of Technology (UTAUT)

UTAUT is a theoretical framework by Davis [17] which combined all models and theories above (TRA, TPB, TAM, DOI, MM, SCT, MPCU) and a combined TPB-TAM model. UTAUT is the latest model in the acceptance of new technologies. Fig. 2 shows the eight factors of UTAUT which are (performances expectancy, effort expectancy, social influence, facilitating conditions, gender, age, experience and voluntariness).

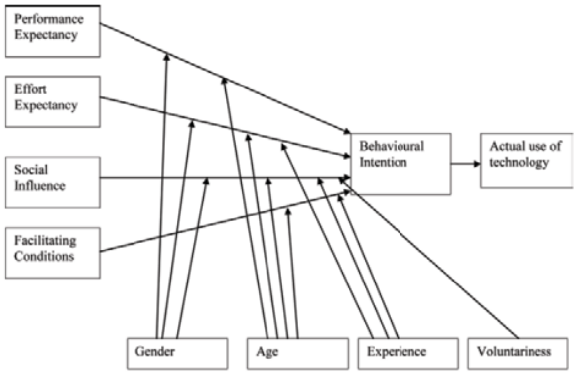

Fig. 2 The eight factors of UTAUT[17]

IV. Conclusion and Future Work

Securing e-government services is depending on technical and non-technical factors. Many researches were trying to apply these models to achieve a high security level for e-government services. However, there is a lack of covering non-technical factors in developing countries. In addition, there is no model covers all these factors. In future work, the author suggests creating a comprehensive security model that can cover the most important technical and non-technical factors in the same time. This suggested model will also take the most useful features of current models together with new approaches to make the model applicable to developing countries.

References

[1] G.Yanqing, "E-Government: Definition, Goals, Benefits and Risks", *2010 International Conference onManagement and Service Science (MASS)*, Vol. 1, No. 4,2011, pp24-26.

[2] S. Alateyah,R.M.Crowder, and G. Wills, "Towards an integrated model for citizen adoption of E-government services", *International Journal of Information Technology & Computer Science*, Vol. 6, 2012, pp47-57.

[3] F. Musau, W. Cheruiyot, and J.C. Mushi, "Trust and Its Challenges Facing E-Government Programs in Kenya", *2011 International Conference onComputer and Management (CAMAN)*,2011, pp1-4.

[4] M. AlNuaimi, K. Shaalan, M. Alnuaimi, and K. Alnuaimi, "Barriers to electronic government citizens' adoption: A case of municipal sector in the emirate of Abu Dhabi" *Developments in E-systems Engineering (DeSE)*,2011, pp.398-403.

[5] S. Shareef, "Electronic government adoption based on citizen-centric approach in regional government in developing countries: the case of Kurdistan Region of Iraq (KRI)", PhD thesis, University of East London, 2012.

[6] M. Rehman, and V. Esichaikul, "Factors influencing the adoption of e-government in Pakistan," *2011 International Conference on E-Business and E-Government (ICEE)*, 2011, pp1-4.

[7] G.Karokola, S. Kowalski, and L. Yngstrom, "Evaluating a Framework for Securing E-Government Services - A Case of Tanzania", *2013 46th Hawaii International Conference on System Sciences*, 2013, pp1792-1801.

[8] J. S. Park,andM.Pokharel, "Issues of Interoperability in E-Govemance System and its impact in the Developing Countries : A Nepalese Case Study," *ICACT 2009 Advanced Communication Technology*, Vol. 3, 2009, pp2160-2164.

[9] JE. Lee, JO. Lee, And S. Sang, "E-Government Challenges in Least Developed Countries (LDCs): A Case of Cambodia," *ICACT 2009 Advanced Communication Technology*, Vol. 3,2009, PP2169-2175.

[10] A. M. Odat, "E-Government in developing countries: Framework of challenges and opportunities", 2012 *International Conference for Internet Technology and Secured Transactions*, 2012, pp578-582.

[11] Z. Ismail,andM.Shajari, "A Comprehensive Adoption Model of e-Government Services in Developing Countries", *2010 IEEE International Conference on Advanced Management Science (ICAMS)*, Vol. 2, 2010, pp548-553.

[12] J. Jing, and S. Meihui, "Analysis of Security Models Based on Multilevel Security Policy", *2012 International Conference on Management of e-Commerce and e-Government*, 2012, pp. 95-97.

[13] S. Al-Azazi, "A Multi-layer Model for e-government Information Security Assessment", PhD thesis, Cranfield University,2008.

[14] F. Al-sobhi, "The Roles of Intermediaries in the Adoption of E-Government Services in Saudi Arabia", PhD thesis, Brunel University, 2011.

[15] S. J. Alotaibi, and M. Walad, "Towards a UTAUT-Based Model for Studying the Integrating Physical and Virtual Identity Access Management Systems in E-Government Domain", *2012 International Conference For Technology And Secured Transactions.*2012, pp453-458.

[16] G. Johanson, and J. Styen, "ICTs and Sustainable Solutions for the Digital Divide: Theory and Perspectives", IGI Global, ISBN 978-1-61520-800-5, 2011.

[17] B. Davis, D. Davis, G. Morries, and V. Venkatesh, "User acceptance of information technology: toward a unified view", MIS Quarterly. 2003, Vol. 27, No. 3, pp425-478.