CONTEXTUAL ADAPTATION OF A SECURITY FRAMEWORK

Anthony Ijeh[1a], Ahmad Al Dahoud[2], Babatunde Ali Alao[3], Stephen .A. Reames[1b]

College of Business Administration, A'Sharqiyah University, Ibra, Sultanate of Oman[1]
Faculty of Information Technology, Jordan University of Science and Technology, Jordan[2]
School of Architecture Computing and Engineering, University of East London, UK[3]

aijeh@asu.edu.om[1a], black4online@yahoo.com [2], ali.alao@ieee.org[3], sreames@asu.edu.om[1b]

Abstract

This paper presents a conceptual framework which has been adapted to use location based service and Wi-Fi technology. This paper will therefore consider and define the issues with the use of the technologies and models by introducing the context of the conceptual framework in Section 1, the exploratory investigation in Section 1.1, the users profiles in Section 2, the contextual adaptation in Section 3, the performance levels of the conceptual framework in Section 4 and a summary of the findings in Section 5.

Keywords - Contextual, Real Time, Security, Framework, User Profiles

1 CONTEXT OF CONCEPTUAL FRAMEWORKS

This paper describes the development of a conceptual framework and aims to provide clear links from existing literature to inform the research design and contribute to the trustworthiness of experimental study. Research studies report that when utilising a conceptual framework, the framework should be considered as a construction of knowledge bounded by the life-world experiences of the person developing it and should not be attributed a power that it does not have [1]. Others state that no researcher could expect that all data would be analysed using a framework without the risk of limiting the results from the investigation [2]. The researchers also stated that by considering these cautions, they hoped they could remain open to new or unexpected occurrences in data and the investigation more generally [2]. Data from experimental reports argue that one of the difficulties typically encountered in the emergence of a new conceptual framework is the use of terms [1].

Figure 1.0 outlines the challenges that every thinking person repeatedly confronts in the course of assembling knowledge from daily life [3]. A study by Olaisen states that everyone navigates sensitively through four domains. The first is the domain of what we know that we know. The second is the domain of what we know that we don't know. Navigating the third domain is more problematic, since it requires us to work with what we don't know that we know. Navigating the fourth is the even more difficult, the domain of what we don't know that we don't know [3]. The conceptual framework developed in this paper used existing technology and security standards by the International Standards Organisation to provide a security framework to mitigate the risks caused by electromagnetic radio wave leakage in wireless networks [4,5].

1.1 Exploratory Investigation

Existing literature describes how encryption can be breached by code crackers [6]. In order to mitigate the risks to wireless networks from electromagnetic radio wave bleeding, the framework being developed uses five logical components [7]. First is the user which is the subject to be located through a mobile device during the interaction with the business Application. Secondly the business application is that which an internet service provider (ISP) offers resources such as web services. Thirdly the mechanism of control is the component responsible for the evaluation and the enforcement of security policies. Fourth is the location middleware (LM) which manages the low-level communications with the location provider, the privacy preferences of the user and the location accuracy requested by the mechanism of control. Lastly the Location Provider (LP) which manages the sensing technologies to provide location measurement of the user to the location middleware [7].

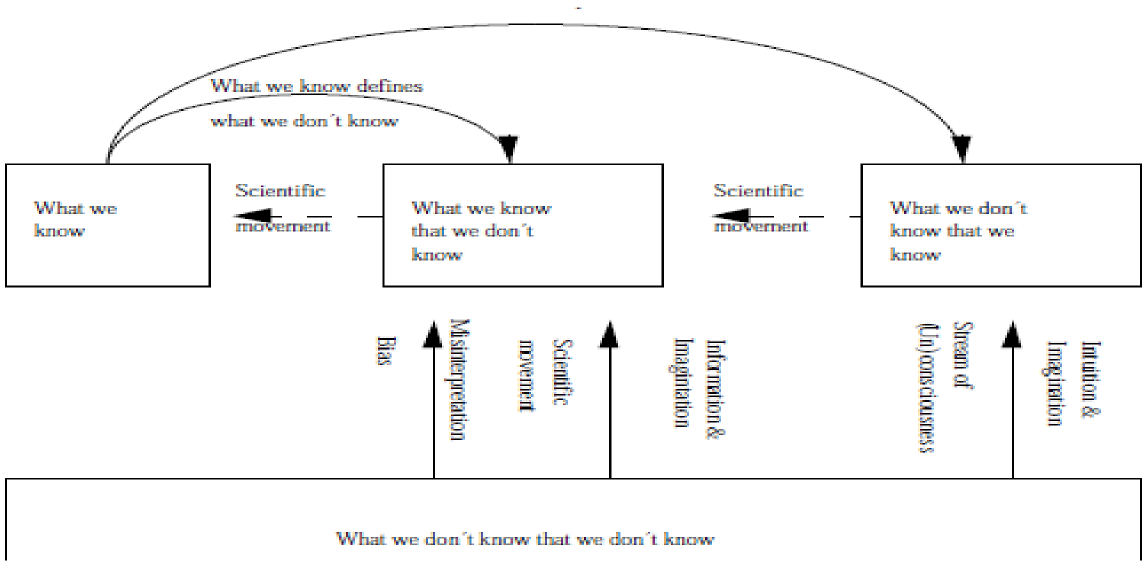
What we know defines
what we don´t know
What we know
Scientific movement
What we know that we don´t know
Scientific movement
What we don´t know that we know
Bias
Misinterpretation
Scientific movement
Information & Imagination
Stream of (Un)consciousness
Intuition & Imagination
What we don´t know that we don´t know

Figure 1.0: The scientific extension of human knowledge [3]

The five logical components described combine together to form networked processing devices that can be distributed to electronic environments that are sensitive and responsive to the presence of people [7]. A different research study confirmed that the logical components interacted autonomously with each other with very little central control and described conventional security models as inadequate for regulating access to data and services used by these logical components [8]. More recently it was found that these logical components fail to take into account the variability, correlation and uncertainty of the context variables composing a security policy when making a security decision [8]. It was further stated that because of these flaws developing a conceptual framework would raise issues of control, trust and privacy and described the issues as interrelated [9]. Table 1.0 shows the outcome of the debate as any framework to be developed would have to mitigate the risks to the logical components and issues described by Sanchez and Perusco [8,9]

Table 1.0: Positives and negatives of LBS for different user types [9]

User Type	Positives	Negatives
Voluntary user. The most likely type, probably using commercial applications such as in vehicle routing and navigation	• Choice • Safety • Convenience • Security	• Security risk • Privacy risk • False sense of security
Mandatory user. Possible in the form of government applications (e.g. home imprisonment) and domestic applications (e.g. tracking minors).	• Safety • Accountability • Security of society	• Invasion of privacy • Security risk • Decreased autonomy • May give users a false sense of security • May give society a false sense of security
Non-user. Unlikely to be a large group if LBS become widespread. Many in this category would have personal reasons for not adopting LBS, or could not afford to use the technology.	• Privacy • Autonomy • Simplicity	• Safety risk • Security risk • Risk of prejudice

2 USER PROFILES

One key area in the conceptual framework is the user profile. The user profile determines the navigation environment, user type and activity. The user profile is dependent on the user's location which is used to grant access. The positioning device specifications are made up of the logical components which provide the service. Using Table 1.1 a researcher reported how the user profile could determine user preferences and privacy settings [10].

Table 1.1: User Profile parameters [10]

Positioning Device Specifications	**Navigation Environment**	**User Activity Type**	**User Type**
Logical components	In-Door	Dynamic and Static	Commercial or Government

The second key area in the conceptual framework is its logical development. The logical components form the core components of the framework. The development is not a build but rather an application of the logical components in a different way to what exists. The aim of the framework is to demonstrate that in using a user's location as a holistic access control mechanism it is possible to protect the physical layer of the Open System Interconnectivity (OSI) model. Within the limits of this papers experiment, the evaluation criteria is based on the ability of the logical components to successfully monitor, grant and decline access to a mobile device. RFID localisation schemes are commonly used.

They are classified according to their approach to a problem. Some of them require the deployment of reference tags which provide finer data but also considerably increase the cost of the system and the maintenance except two schemes that are built on very specific properties of passive tags. The next key area in the conceptual framework is the security strategy development. The aim is to identify the impact, probability, and preparedness of information security strategies and rate them. The ISO 27001:2005 standard to be used in continuously improving the security solution was found to have low adoptability in SMEs as shown in Table 1.2.

Table 1.2: ISO ISMS guides applicability to SME's [11]

Name of Standard	**Company Size**	**Creation**	**Necessity**	**Cost in money**	**Skills Needed**	**Language Issues**
BS 7799-1 & 2	Civil Service & Big Company	1995	Not Mandatory	N/A	Standard Level	English
ISO 27001 (BS 7799-2)	Civil Service & Big Company	2005	ISO Certification Possible	N/A	Standard Level	International
ISO 27001 (BS 7799) – (BS 7799 – 1)	Civil Service & Big Company	2005	Standard Only	N/A	Standard Level	English

3 CONTEXTUAL ADAPTATION OF REAL TIME FRAMEWORKS

The intention of this section is to develop and present a framework that can be used to mitigate the security risks caused by the leakage of electromagnetic radio waves in wireless networks using a prototype. The user profile is the entity that is located as a mobile device. The users profile is defined by the security model and authenticated by the security solution in order to gain access to the web service application. Only mobile devices with specifications and functionalities that meet the requirements of the security strategy model can obtain access to the web service application. The Location Based Service (LBS) communicates with the mobile device which is setup with sensors to send and receive signals within a physical space. The LBS is able to manipulate the data from the mobile device because of the set of instructions in the user's profile. The LBS uses the specific position or point in physical space to ascertain the mobile devices relative position and movement within defined parameters. The security solution uses an algorithm to control access rights and receives alerts from the location based service at set intervals on the mobile devices position. The security solution is designed to take into account the flaws of information it receives from the LBS which are the error margin of the exact location of the mobile device and the reporting time variance from when the mobile device was at a position which could have moved and the time of reporting the position.

4 PERFORMANCE LEVELS

The frameworks strategy model was evaluated using a questionnaire to collect data from Small Medium Enterprises (SME) which use wireless networks to understand the kind of infrastructure they use and the kind of information security policies they have in place to protect them. This enabled the study identify the various security related perceptions held by executive and functional personnel and the degree to which these perceptions are similar using enterprises that are of a similar size for consistency. The results were compared with surveys undertaken by PricewaterhouseCoopers (PwC) on behalf of the United Kingdom's Government office of Commerce (GOC) which produced the ISO 27001:2005 and ITIL V3 documents. The strategy model performance target was set at 95% confidence levels for compliance and implementation against the Governments independent survey [12]. The security solution was evaluated using a laboratory owned by a company that provides Location Based Services to the National Health Service (NHS). The results were compared with a predetermined route marked out on the architectural plan of a room in the laboratories building which was used as a test bed. The security solutions models performance target is set at 95% confidence levels for accuracy and precision using the marked route [13]. Based on statistical analysis using the 95% confidence interval provides assurance that the performance levels of the security strategy and solution are performing as expected [14].

5 SUMMARY

This paper has presented a conceptual security framework by describing the main techniques of developing a security framework. The paper provided a privacy focused access control framework to mitigate the risks to electromagnetic radio waves. In building the framework the paper used the technologies and models discussed in the literature. A preliminary experimental investigation was undertaken to understand the drawbacks of using the technologies and models before looking at the user's profiles. The paper then presented the solution and strategy models and their expected performance levels. The confidence interval is set at 95% so that if the performance level is less than 95% then the security solution and strategy are to be rejected.

6 REFERENCES

[1] Friedman, K (1998): Building Cyberspace in Information, Place and Policy. C. Ess and F. Sudweeks (Eds). Proceedings of the Cultural Attitudes towards ICT, University of Sydney Australia, p51-78. [Online] Available at: http://www.it.murdoch.edu.au/~sudweeks/catac98/pdf/05_friedman.pdf [Accessed 20th of July 2011].

[2] Miles, M. B. & Huberman, M. A. (1994): Qualitative Data Analysis: An Expanded Sourcebook (2nd Edition), Beverley Hills: Sage. ISBN-13: 978-0803955400. [Online] Available at: http://www.mendeley.com/research/qualitative-data-analysis-an-expanded-sourcebook-2/ (Login required) [Accessed 20th of July 2011].

[3] Olaisen, J. (1996): Information, cognitive authority and organizational learning, in Olaisen, J., Wilson, P. and Munch-Pedersen, E. (Eds), Information Science: from the Development of the Discipline to Social Interaction. Oslo: Scandinavian University Press, p. 7-19.

[4] Ijeh, A.C., Brimicombe, A.J., Preston, D.S., Imafidon, C.O. (2009): Security Measures in Wired and Wireless Networks. In Proceedings of the Third International Conference on Innovation and Information and Communication Technology (ISIICT'09) held at the Philadelphia University, Amman, Jordan, 15th – 17th December, 2009: Published by the British Computer Society, Swindon, UK, p1-10. [Online] Available at: http://dl.acm.org/citation.cfm?id=2228043 [Accessed 20/02/13]

[5] Ijeh, A.C. Preston, D.S. Imafidon, C.O. Watmon, T.B. Uwaechie, A.O. Ojeme, S. Lucas, B.R. (2010): Geofencing Engineering Design and Methodology: IAENG International Conference on Operations Research (ICOR). Royal Garden Hotel, 17th-19th March, 2010: p2157-2162. ISBN: 978-988-18210-5-8 [Online] Available at: http://www.iaeng.org/publication/IMECS2010/IMECS2010_pp2157-2162.pdf [Accessed 20/7/11].

[6] Wong, S. (2003): The evolution of wireless security in 802.11. SANS InfoSec Reading Room - Wireless Access, 1 (1), p1-12 [Online] Available at: http://www.sans.org/rr/whitepapers/wireless/1109.php [Accessed 20th of July 2011]

[7] Ardagna, C.A. Cremonini, M. Vimercati, S.D.C Samarati, P. (2009): Access Control in Location-Based Services. Privacy in Location Based Applications, C. Bettini, S. Jajodia, P. Samarati, and S. Wang (Eds.), Springer, 2009, p106-126. ISBN: 978-3-642-03510-4

[8] Sanchez, S. M. (2007): Work smarter, not harder: guidelines for designing simulation experiments. In Proceedings of the 39th conference on Winter simulation: 40 years! The best is yet to come (WSC '07), IEEE Press, Piscataway, NJ, USA, p84-94. ISBN: 1-4244-1306-0

[9] Perusco, L. Michael, K. Michael, M.G (2006): Location-Based Services and the Privacy-Security Dichotomy. Proceedings of the 3rd International Conference on Mobile Computing and Ubiquitous Networking, p1-8

[10] Al-Nabhan, M. M. (2009): Adaptive, reliable, and accurate positioning model for location-based services. Brunel University Research Archive (BURA), November 2009. School of Engineering and Design, PhD Theses, p1-234. [Online] Available at: http://bura.brunel.ac.uk/handle/2438/3963 [Accessed 20th of July 2011].

[11] Barlette, Y. and Fomin, V. V. (2008): Exploring the Suitability of IS Security Management Standards for SMEs. Proceedings of the 41st Annual Hawaii International Conference on System Sciences in IEEE Computer Society Journal, USA, p1-10. ISBN: 0-7695-3075-3. [Online] Available at: http://dx.doi.org/10.1109/HICSS.2008.167 (login required) [Accessed 20th of July 2011].

[12] Ijeh, A.C. Ali-Alao, B. Preston, D.S. Imafidon, C.O. (2011) Quantitative Analysis of ISO/IEC 27001 Security Policies: The 1st IEEE Conference on Communication, Science & Information Engineering, (CCSIE). Middlesex University, London 25th – 27th, 2011: p183-186, ISBN: 978-0-9556254-5-9 [CD-ROM] Available at: http://www.ccsie.org/Contact.htm [Accessed 20/7/11].

[13] Ijeh, A.C. Ali-Alao, B. Preston, D.S. Imafidon, C.O. (2011) Simulating Euclidean Distances using Location Based Services: The 1st IEEE Conference on Communication, Science & Information Engineering, (CCSIE). Middlesex University, London 25th – 27th, 2011: p180-182, ISBN: 978-0-9556254-5-9 [CD-ROM] Available at: http://www.ccsie.org/Contact.htm [Accessed 20/7/11].

[14] Field, A (2005): Discovering Statistics Using SPSS (Introducing Statistical Methods series), SAGE Publications Ltd, p1-816. ISBN: 9780761944515

ACKNOWLEDGEMENT: Presentation of this paper was made possible by funds provided by the College of Business Administration (COBA) and Vice Chancellors Office (VCO) at A'Sharqiyah University.