The Technological Hybrid of Geofencing Engineering

Anthony .C. Ijeh, David .S. Preston, Chris .O. Imafidon, Titus .B. Watmon, Annette .O. Uwaechie,
Martin Cooke, Peter Lancaster, Andy Widdess, *Member IAENG*

***Abstract*—The focus of this paper is a review of a unique hybrid security concept which provides an intervention to a real world problem; the intervention provides security to the medium for wireless networks as a result of leakage which occurs when radio magnetic waves are used by wireless networks to carry data. The findings of our review showed that the hybrid security concept can be used to provide the intervention once crafted in an appropriate manner. The variables obtained from the review done in this research paper enabled an experimental proof of concept (POC) to be undertaken; the POC was funded by a grant from the worshipful company of haberdashers, England**

***Index Terms*—Location Based Service, Radio Frequency Identity, Security Strategy Models, Wireless Fidelity**

I. INTRODUCTION

In the preceding papers to this [1]-[9] a complete review of relevant literature covered the topics without being confined to one research methodology, one set of journals or one geographic region [10]. Sharing this viewpoint, the literature review presented in this paper covers all existing Security Strategy Models, Location Based Service Models, Radio Frequency Identity Models and Wireless Network Models. As shown in Fig 1. The strategy's aim was to ensure that the literature being reviewed and used was not confined to one methodology, covered all literature related to the thesis, covered various journals rather than just one, covered journals from various continents

Manuscript received (January 1, 2010). This work was supported in part by a grant from the Worshipful Company of Haberdashers UK and the free use of a Location Based Service Laboratory owned by AireTrak Ltd based At Huntingdon in the UK

A .C. Ijeh was with RSM Tennon, LLP, UK. He is now an Information Security Researcher with the University of East London, 4 – 6 University Way, London, E16 2RD, UK (Corresponding authors phone: +44(0)208-223-7778; e-mail: ijehanthony@yahoo.co.uk)

D .S. Preston is with the University of East London, 4 – 6 University Way, London, E16 2RD, UK (e-mail: d.preston@uel.ac.uk)

C .O. Imafidon is with the University of East London, 4 – 6 University Way, London, E16 2RD, UK (e-mail: c.o.imafidon@uel.ac.uk).

T .B. Watmon is with the University of East London, 4 – 6 University Way, London, E16 2RD, UK (e-mail: bt.watmon@gmail.com)

A .O. Uwaechie is with Zenith Bank PLC (e-mail: Annette.Uwaechie@zenithbank.com)

M. Cooke is with Angle Technology PLC based at Surrey (email: M.Cooke@angleplc.com)

P. Lancaster is with the National Physical Laboratory (email: peter.lancaster@npl.co.uk)

A. Widdess is with the Location Based Service Laboratory of AireTrak Ltd (email: andy.widdess@airetrak.com)

II. THE TECHNOLOGICAL HYBRID

In order to present our proposed solution for leakage Wi-Fi networks we have selected a few research papers by authors of comparable academic standing who have specialised in the area of Geofencing for review before discussing other research papers that further highlight the framework as a possible solution to the leakage in Wi-Fi networks. With this in mind the authors have asked the all important question can a laptops location position be used to control its access to a wireless network by using a pre-determined path route. The proposed model presented is similar to the model used by; [11] but different in that it focuses on the technological elements of LBS transactions. Table I shows the variables used to develop the Threat model for the Location Based Service security and the Trust Model for Location Based Services in Table II

III. WIRELESS LOCAL AREA NETWORKS (WLAN)

Contemporary research has linked most issues arising in wireless communication to the privacy and security of confidential information [12]**.** This is due to data from wireless networks being transmitted between devices through the air via radio waves, which are susceptible to interception from unauthorised persons. Solutions have been sought for these problems with the emergence of IT Governance and new security protocol. As radio waves are used as a medium it is more difficult to contain signals within an organisations physical boundaries or a defined area. Further more because the data is not travelling via a wired network, it is always possible for an unauthorised person to intercept it without being within the organisations physical boundaries or being attached to the network. This means that organisations cannot control data that is transmitted over a wireless network.

IV. SECURITY STRATEGY MODEL (SSM)

Security strategies in Geofencing are categorised by the classification of positioning systems / architectures falling under the following categories; Indoor e.g. WLAN and Outdoor e.g. GPS; Some of the most interesting positioning application areas have emerged in Wireless Communications. The most prominent are the FCC (Federal Communications Commission) which requires that the precise location of all enhanced 911 (E911) emergency calls be automatically determined and the European Recommendation E112. Both E911 and E112 require that wireless providers should be able to locate within tens of meters users of emergency calls. Localisation Algorithms include the Time-Of-Arrival (TOA), Time-Difference-Of-Arrival (TDOA), Direction-of-Arrival

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

(DoA) also known as Angle-of-Arrival (AoA) and Received Signal Strength (RSS). The security strategies are decided by the wireless carriers who use the mandates E112 or E911 and the techniques they have available to them to monitor and transmit data using Wi-Fi networks [13].

V. LOCATION BASED SERVICES (LBS)

In order to evaluate our proposed solution to the leakage in Wi-Fi networks we selected a few research papers by authors of comparable academic standing who had specialised in the area of Location Based Service Models for review. Our findings showed that one unique model used an immersive virtual reality (VR) based approach for capturing data in real time on information transactions and individual behaviour in a dynamic controlled environment. We also found that the model used a questionnaire to gain an understanding of each LBS user's spatial ability. Furthermore the models application allowed a wireless device usage which was recorded along with the track taken by individuals in the experiment. However the study acknowledges its limitations as being the movement of the wireless device which is directed by a joystick rather than the actual movement of an individual; this is considered a limitation in replicating the real world [14]-[17]. However responses to the post-experiment questionnaire showed that the way finding behaviour in VR did indeed accord with their usual real world behaviour. This paper proposes the use of the security issues faced by large and medium registered companies in the UK collected by a designed questionnaire and developed into a security risk model. This paper also proposes the use of the actual movement of wireless devices by individuals in a controlled environment that can be tracked and monitored and whose data can be collected and fed into the security risk model in order to understand the current, emerging and real threats faced by the companies using wireless networks in the UK. Finally this paper proposes the use of this risk model to develop a trust model that can be used to mitigate the risks to privacy in wireless network data transmission. Fig 2 was developed using the risks to security whilst adopting previous models

VI. RADIO FREQUENCY IDENTITY (RFID):

Most location based services (LBS) use Radio frequency identity (RFID) technology to monitor devices within predefined parameters. The combination of both technologies has led to increased interest in the area of Dead spots which are areas of none activity within predefined LBS areas or test beds. Using a Proof of concept approach this section aims to identify and discuss the spots of reach and inactivity within a Location Based Services environment. In order to do so we use a live LBS environment to monitor Radio Frequency Identity tags (RFID) attached to a wireless mobile device. By so doing the flight of the tag is monitored using a predetermined path as well as that of the wireless mobile device (laptop) which is monitored using its MAC address. [18]. Even with its growing use and adoption RFID technology still has set backs such interference from Noise this study will use a live LBS environment to emulate some of these interferences and show how they can affect the flight of the tag. Table III shows RFID functions

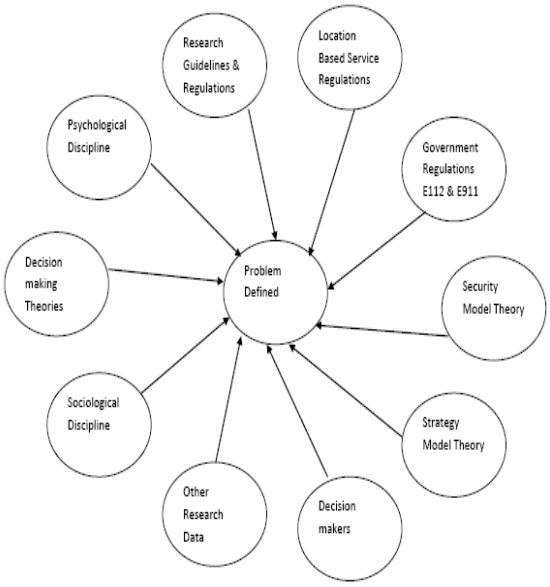

Fig 1: Areas of Interest in the Literature Search

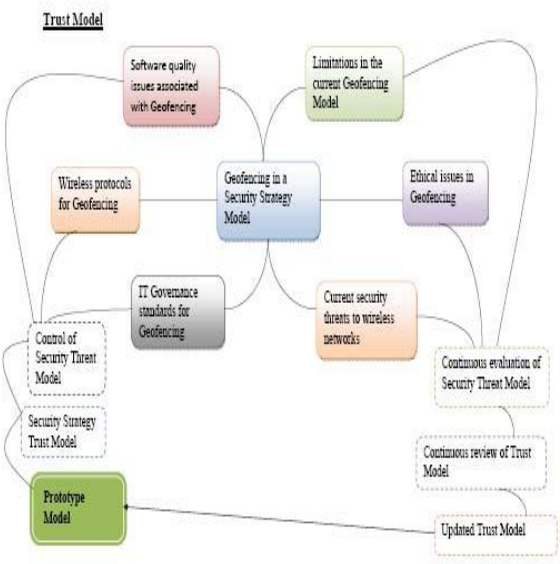

Fig 2: Geofencing Trust Model for wireless Security

VII. LOCATION AS A UNIQUE IDENTIFIER OF ACCESS

Having discussed the background literature of the areas used to address leakage in Wi-Fi networks we have selected a few research experiments by authors of comparable academic standing who have specialised in the area of using Location as a Unique Identifier of Access Control for review before discussing other research papers that further highlight the generic framework as a possible solution to the leakage in Wi-Fi networks. Before doing so we look at the three methods used in Wi-Fi networks for location as a Unique Identifier of Access Control and also look at their advantages and disadvantages. Table IV, shows LAN methods with benefits and disadvantages of each method

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The request for positioning is sent by the LBS provider to a positioning services provider (PSP) whose function is to contract and liaise with network and technology providers so as to perform the position fixing of targets. A range of services can then be provided from thereon and they include the data in Table VI. The Implications of using Location as a Unique Identifier of Access Control affects the robustness of their applications and pose challenges to Geofencing Engineering; these include the data in Table V. Against the backdrop of Table V and Table VI, this paper looks at how other author's have applied Location Based Services

Table I: Dependent and Independent Variables of LBS Threat Model

Dependent Variables	**Data Measure of Dependent Variable**	**Independent Variables**	**Data Measure of Independent Variable**
RFID Technology	Compliance with EU & IEEE Standards	Signal corruption, Data, GIS software, spatial relationships, Projection, scale, data format, metadata, radio transmission	RFID Infrastructure used for live test
Test bed	Compliance with EU Metric Measurement standards	Volume of the floor of the library, Volume of the Ceiling of the library, Volume of the Walls of the library	Volume of Test bed during live test
Wireless Communication System	Compliance with IEEE Protocols	Direct or reflected signals, algorithms, software engines, Specification	WCS Infrastructure used for live test
Access Points	Compliance with IEEE protocols	Range, RSSI, RSS, Signal strength, radio waves, reach	Received Signal Strength Indicator
Mobile Wireless device	Compliance with EU Manufacturing standards	Specification	Functionality of Laptop during live tests
Noise & Interference	Compliance with EU & IEEE Recommendations	Interference	Noise during live tests

Table II: Dependent and Independent Variables of LBS Trust Model

Dependent Variables	**Data Measure of Dependent Variable**	**Independent Variables**	**Data Measure of Independent Variable**
Trust Model	Mitigation of Threat Model	Geofencing Prototype Application	Ability to Secure Wi-Fi Network

Table III: Radio Frequency Identity Tags

Functionality	**Passive tag**	**Active tag**
Power	No direct power, obtain power through radio signals transmitted by RFID readers	Own power supply e.g. equipped with battery
Memory	Small size memory that stores limited information such as ID	Large memory for storing data and processing information
Range	Short communication range within a few meters	Long range e.g. tens of meters

Table IV: Local Area Network positioning techniques

Method	**Advantage**	**Disadvantage**
Triangulation	Increased accuracy and more robust	Not reliable in indoor areas that use multi-path environments
Direction		Not reliable in indoor areas that use multi-path environments
Finger print	Uses received signal strength pre- stored on a database. Far easier to obtain than the other methods	

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Table V: Implications of using Location as a Unique Identifier of Access Control

Challenge	**Implication**
Data	Data handling and timely response to queries, maintaining the currency of data, type of data will determine the database structure
Locating User	The number of different ways in which a users location can be expressed, and the accuracy sufficiency in determining the position of the user
Context	Situational context which adopts risk and doesn't look at the users gender
Spatial Query	Query processing times and the user applicability representation
Communication	Screen size can make delivery of data unintelligible
Interoperability	The hybrid that is Geofencing Engineering can lead to the interoperability of the different technologies
Legal and Social Issues	Notions of privacy and being able to track users through their profiles
Business Model	Security Strategy Models which provide security to business data but are currently not featured strongly in Geo-Information

Table VI: The range provided of services by Location Based Services

Activity	**Application Area**
Navigation	Car navigation systems e.g. real time traffic updates
Way Finding	Routes and modes of transport
Real-time Tracking	Tracking children in the playground
Mobile Commerce	Transactions by persons on the move
User-solicited information	Social purposes e.g. weather forecasts
Location based tariffs	Pay-as-you-go car insurance schemes
Fulfillment	Data collection e.g. Geofencing
Co-ordinating	Emergency services e.g. responding to disasters
Artistic expression	Location based story lines
Mobile gaming	Location based games and their players

VIII. CONCLUSION

In this paper we provide an introduction to the Technological hybrid of Geofencing Engineering (GE). In so doing this paper looks at the use of various security concepts to form a technological hybrid; which is then used to provide an intervention. The security concepts used include a Security Strategy Models, location based service technology, Radio Frequency Identity, Wireless Communication technology, Access Points, Noise and Test beds. The review suggests the applicability of the security concept and its compliance with existing regulatory standards as acceptable. This review was an introduction to the gaps in knowledge of wireless network security and not a demonstration of the prototype experiment used to fill the gap

REFERENCES

[1] Ijeh A.C; Brimicombe, A.J; Preston, D.S; Imafidon, C.O; Uwaechie, A.O; (2009) "Using Geofencing to Overcome Security Challenges in Wireless Networks: Proof of Concept" In proceedings of the Information Society 12th international multi-conference 12-16 October 2009, Ljubljana, Slovenia http://is.ijs.si/is/is2009/zborniki/Zbornik_A.pdf

[2] Ijeh A.C; Preston, D.S; Imafidon, C.O (2009) "Geofencing in a Security Strategy Model" ICGS3'09 (formerly ICGeS) Conference Proceedings 1st to the 2nd of September 2009 www.springerlink.com/index/p85j16w581444106.pdf

[3] Ijeh A.C; Preston, D.S; Imafidon, C.O (2009) "The Significance of Security in transmitting clinical data" ICGS3'09 (formerly ICGeS) Conference Proceedings 1st to the 2nd of September 2009 www.springerlink.com/index/t5575533t1341601.pdf

[4] Ijeh A.C; Preston, D.S; Imafidon, C.O; (2009) "Aggravating Wireless Protected Access II (WPA 2)" IN the International Journal of Security Volume 3, Issue 4; Published by the Computer Science Journals Kuala Lumpur, Malaysia September 2009 www.cscjournals.org/Journals/IJS/volume3/Issue4/IJS-15.doc

[5] Ijeh A.C; Brimicombe, A.J; Preston, D.S; Imafidon, C.O; (2009) "Security Measures in Wired and Wireless Networks" In proceedings of the 3rd International Symposium on Innovation in Information & Communication Technology 15 - 17 December, 2009, Philadelphia University, Amman, Jordan (ISIICT 2009) http://www.bcs.org//upload/pdf/ewic_iict09_s4paper2.pdf

[6] Ijeh A.C; Brimicombe, A.J; Preston, D.S; Imafidon, C.O; (2009) "Evaluating Ethical and Productivity Issues in Geofencing" Symposium on progress in Information and Communication Technologies 7-8 December 2009 Kuala Lumpur, Malaysia (SPICT 2009) http://spict.utar.edu.my/SPICT-09CD/contents/pdf/SPICT09_A-1_1.pdf

[7] Ijeh A.C; Preston, D.S; Imafidon, C.O (2009) "Evaluating Location Based Privacy in Wireless Networks" In the proceedings of the 4th Annual Advances in Computing Technology Conference

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

(AC&T). 27th of January 2009, page 142-150. University of East London http://www.uel.ac.uk/act/proceedings/documents/FinalProceedings.pdf

[8] Ijeh A.C; Preston, D.S; Imafidon, C.O; Williams, G (2009) "Security Strategy Models (SSM)" In the proceedings of the 4th Annual' Advances in Computing Technology Conference (AC&T) 27 January 2009, pp 126-131. University of East London United Kingdom http://www.uel.ac.uk/act/proceedings/documents/FinalProceedings.pdf

[9] Ijeh A.C; Preston, D.S; Imafidon, C.O, Watmon, T.B (2010) "The Context of Geofencing Engineering" 2010 International Conference on e-Commerce, e-Administration, e-Society, e-Education and e-Technology at the Grand Lisboa, Macau, China January 25 – 27, 2010 http://e-case.org/2010/

[10] Webster J & Watson RT (2002) analysing the past to prepare for the future: writing a literature review; MIS Quarterly 26(2): xiii – xxiii

[11] Jokela, T. and Iivari, N., (2003) Systematic Determination of Quantitative Usability Requirements. To be published in the proceedings of HCI International 2003, (Crete, 2003).

[12] Ijeh A.C; Preston, D.S; Imafidon, C.O (2009) "The Significance of Security in transmitting clinical data" ICGS3'09 (formerly ICGeS) Conference Proceedings 1st to the 2nd of September 2009 www.springerlink.com/index/t5575533t1341601.pdf

[13] Brimicombe, A.J and Li, C (2009) Location Based Services and Geo-Information Engineering (Accessed: 20/06/09) http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470857366.html

[14] Golledge, R.G., and Stimson, R.J., (1997) Spatial Behaviour: A Geographic Perspective, the Guildford Press, New York 1997

[15] Blades, M., Lippa, Y., Golledge, R.G., Jacobson, R.D., and Kitchin, R.M. (2002) Way finding by people with visual impairments: The effect of spatial tasks on the ability to learn a novel route. Journal *of Visual Impairment and Blindness* 96, 407-419.

[16] Li, C (2005) "User preferences, information transactions and location-based services: A study of urban pedestrian way finding" in Computers, Environment and Urban Systems Science Direct, Elsevier 30 (2006) 726–740, assessed from www.elsevier.com/locate/compenvurbsyson 9/8/08

[17] Jokela, T. and Iivari, N., (2003) Systematic Determination of Quantitative Usability Requirements. To be published in the proceedings of HCI International 2003, (Crete, 2003)

[18] Brimicombe, A.J and Li, C (2009) Location Based Services and Geo-Information Engineering (Accessed: 20/06/09) http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470857366.html

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)