Security Measures in Wired and Wireless Networks

Anthony C. Ijeh¹, Allan J. Brimicombe², David S. Preston¹, Chris .O. Imafidon¹

¹ School of Computing and Technology, University of East London, UK

² Centre for Geo Information Studies, University of East London, UK

University of East London, 4 – 6 University Way, London, E16 2RD, England, United Kingdom

ijehanthon@yahoo.co.uk, a.brimicombe@uel.ac.uk, d.preston@uel.ac.uk and c.o.imafidon@uel.ac.uk

Abstract

The purpose of this study is to review contemporary wireless network protocols and areas that affect the ability of wireless fidelity (Wi-Fi) technology to secure data transmitted over wireless networks. The research approach takes the form of a case study, in collating the methods used by existing protocols in the implementation of wireless Security Trust Models within their networks. So the paper follows a case study methodology on all the wireless protocols provided by the Institute of Electrical and Electronic Engineers

Wireless protected access Wi-Fi protected access; version 2 (WPA2) protocol has provided a more secure means for securing wireless networks but has only provided stronger encryption as it has a longer key which takes longer to decipher. So far, researchers have acknowledged that location privacy is critical to the security of data transmitted by wireless technology.

The security reality though, is that even with the implementation of the purportedly secure standards for wireless systems e.g. the 802.1x suite; there are insecure gaps where the information in transit remains in its plain unprotected form for some seconds before it is re-encrypted into another format for transmission. It is at such security holes that the information criminals tend to attack.

In this paper, we identify the various security related challenges faced by wireless protocols. This study is useful as it provides lessons for ICT managers, directors, academia and organizations, who wish to develop install or are already using wireless networks within their offices

Keywords: Wi-Fi, WPA2, Wireless, Wired, Networks, WEP, Privacy, Security, Protocol, Models

1. INTRODUCTION

A substantial amount of issues arising in wireless communication can be linked to the privacy and security of confidential information. 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. However the existing protocols are yet to safeguard against the location boundaries of the radio waves transmission; which flows beyond the physical boundaries of the organisation and allows the data to be intercepted by unauthorised persons outside the physical vicinity of organisations using specially equipped laptops.

As radio waves are used as a medium it is impossible 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

The secure use of wireless networks is based on users connecting to the network via predetermined access points using protocols in order to access the network securely. The existing protocols are the wired equivalent privacy protocol (WEP) and the wireless fidelity (Wi-Fi) Protected Access Protocols (WPA or WPA2)

However the protocols still require the use of radio waves as a transmission medium and as such data can be intercepted and used by unauthorised persons. The increased use of Hotspots and Wi-Fi areas in the City of London region, which is densely, populated with financial organisations means that other alternative security arrangements need to be made.

Hence this paper will investigate the use of security as a measure in wireless networks with a view of suggesting a more secure way of granting access and transmitting data using Wi-Fi networks. The research will be of a qualitative nature. The preliminary study has identified 5 areas for review in the annotated bibliography which are: a) Wired Equivalent Privacy Protocol (WEP) , b) Wired and Wireless networks, c)

Privacy, d) Security, e) WPA and WPA2 (protocols). For the purpose of this paper the author has selected 2 journals for each of the 5 areas in that 10 works are reviewed in total.

2. WIRED EQUIVALENT PRIVACY (WEP)

This article, from an academic, peer-reviewed journal specializing in wireless communications, details recent findings on how a practical key recovery attack on Wired Equivalent Protocol (WEP), based on partial key exposure vulnerability in the encryption being used (RC4 stream cipher) can be used as a flaw in breaking WEP. The article describes how to apply the flaw in breaking WEP and concludes that the protocol also referred to as 802.11b WEP standard by the Institute of Electrical and Electronic Engineers Inc, is not secure. Information from this article will help us support our research proposal that suggests current WEP problems which are still being experienced as WEP is still widely being applied by organisations and home users make the use of WEP a threat to the integrity of confidential data held on any network using it as their protocol; Stubblefield, A; et al. (2004)

This article, whose journal has been peer-reviewed originated from, the highly respected engineering department of Stanford University which amongst other things specializes in wireless communications protocols. It details recent findings on how the Wired Equivalent Privacy (WEP) protocol lacks the ability to exchange its encryption keys safely key and has from severe cryptographic issues to the extent that secret service personnel have used public lectures to demonstrate how easy it is to break into a 128-bit WEP key in less than five minutes. The article suggests that it was for these reasons that the IEEE developed the 802.11i Standard in order to boost confidentiality, integrity, and mutual authentication between the keys and thus develop good key management practices. Information from this article will be used to support the research proposal that suggests current WEP protocol is inadequate to in maintaining the security of the wireless networks as it can be easily breached by unauthorised persons; He, C. et al (2005)

2.1 Wired and Wireless Networks

This article, originates from, an ACM International Conference whose researchers are based at the Los Angeles University in the Computer Science department Engineering department. The article suggests that connections using the 802.11 protocol in wireless Local Area Network (LANs) are reasonably good and as such that is what makes them widely used in educational institutions and scientific research laboratories. The study however suggested that the 802.11 protocol was rather unstable with wired networks and was going to investigate why this was so using both the wired and wireless networks. Information from this article will help us produce a more credible research proposal as it objects to the common notion that the WEP protocol is not suitable for wireless technology. We noted that the journal dated back to 2002, which could have been a reason for their opinion, however the study will take on board what has been said; Xu, K. (2002)

This article, originated due to funding provided as a Grant, which was given to the University of Washington and the Microsoft Research Laboratory in a joint collaboration between academics and professionals. It details recent findings on Medium Access Control (MAC) level behaviour of operational wireless networks. The article described the how they had uncovered a picture of MAC operations which suggested that the 802.11 protocol required further study. The picture suggested that networks which were MAC were unnecessarily tuned which led to its inefficient utilisation which were due to MAC backing off more than required in response to negative activity. Information from this article will help us support our research proposal that suggests even though current WEP protocol is flawed, we cannot disregard the protocol as it has not been review long enough; Mahajan, R. (2006)

2.2 Privacy

This article, from an academic, peer-reviewed journal specializing in wireless location privacy, details recent findings on how a practical key recovery attack on Wired Equivalent Protocol (WEP), based on unauthorised person could track a user's position. In addition, they suggest that interface identifiers which uniquely identify each client, allows tracking of locations over time. The study also suggests that by disposing interface identifiers a user's location is kept secret and gave example of how an experiment using an analysis of a public WLAN has already shown this theory to be true. The study supports what was said earlier by Mahajan, R (2006) and also suggests that using MAC is not sufficient and that mechanisms should be rebuilt for privacy. Information from this article will help us support our research proposal that suggests current location of Wi-Fi access cold be used to secure access points and levels for users working with confidential data; Gruteser, M. and Grunwald, D. (2005)

This article, from an academic, journal specializing in wireless privacy, details recent findings on how other users may intercept and read this information. The study describes how there is a need for technical user to have a more accurate understanding of privacy. Information from this article will help us support our research

proposal that suggests the current understanding of privacy is vague as what constitutes privacy in one company is not what constitutes the same in another; Kowitz, B. and Cranor, L. (2005)

2.3 Security

This article is an academic journal and originates from, the Columbus State University. It details recent findings on how different techniques that can be used to strengthen security in wireless local area networks (WLANs). It also discusses the evolution of the WLANs and suggests that the early versions of wireless networks weren't meant to be consumed the way it did. However the article did suggest that the emerging security technology should be implemented in order to combat the threats and that with proper planning one day the wireless would be as secure as the wired. The information in this article will help support our research proposal which suggests that WLANs data transmitted by radio waves exposes the organisation to security risks such that the integrity of confidential data held on any of their networks using the known standards such as 802.11 protocols is not reliable; Bhagyavati et al. (2004)

This article, from an academic, journal specializing in wireless security patches, details recent findings and developments on an educational establishment's specific need. They suggest that the wireless security patches have improved performance of the networks. Furthermore other researchers then suggest that the security patches when applied allow for more band width, which gives the network user increased speed. They go on further to suggest that there is a possibility that the viruses and other malware can distort data and affect wireless environment, as such as its needs to be kept under good management. Information from this article will help us support our research proposal that suggests our assumption will be reduced to a minimum when carrying out the research as the study will attempt to abide with best practices in IT when conducting the research; Higby, C. and Bailey, M. (2004)

2.4 WPA and WPA2 Protocols

This article, from an academic, journal specializing in the WPA and WPA2 Protocol, details recent findings on why the WPA protocol was developed and what vulnerabilities it was created for. The article further describes that the WPA adopted the key management system or Temporary Key Integrity Protocol (TKIP). The article however suggests that the protocol uses keys generated by the server, which even though dynamically created still leave room for the keys to be hacked into. This study acknowledges the use of Message Integrity Checks (MIC) in order to mitigate against the keys being cracked. However, there is still room for unauthorised persons to break into the network via these distributed keys. Information from this article will help us support our research proposal that suggests current the protocols whilst bring a management framework by which the wireless network can be governed cannot provide the required security as there is still signal leakage which allows unauthorised persons to access the organisations network and view confidential data; Hori, Y. and Sakurai, K (2006)

This article, from an academic, journal specializing in Protocol behaviour, details recent findings on why the protocol identification using features left after encryption is useful. The study suggests that this is due to the fact that classified data i.e. which has been encrypted connects with greater accuracy based on single connections. Information from this article will help us support our research proposal that suggests that the current protocols using certain types of encryption will be better off in pin pointing the keys and data to the access points for connection; Wright, C.V. (2006)

3. MODEL ANALYSIS

Modern wireless networks represent new technology which unfortunately retains sufficient deficiencies for enemies to commit old style crimes upon them; Figure 1. In search of adequate security the Institute of Electrical and Electronic Engineers (IEEE) has sought to establish protocols that can guarantee the secure connections to wireless networks (Wong 2003). With this the IEEE has had some success but has not taken on a by product of using wireless networks into consideration; radio wave leakage (Wong 2003). Various researchers have proposed novel projects to be used in securing wireless access points and suggested that they were developed for the next generation.

However new developments were scalable, secure, transparent and simple; have not been easily implemented due to their protocols and protection mechanisms. This has continued to provide unanswered questions such as, how to contain the radio waves leakage of wireless communication systems (Friday, Wu et al. 2003)

In comparison to this some researchers have suggested that there might be the feasibility of launching and detecting jamming attacks in wireless networks. The objective of these jamming devices was to interfere with the signals of the radios electromagnetic waves and cause disruption. These jamming attacks were developed into models and used to disrupt air time of network users or block them out completely (Xu, Trappe et al. 2005). What the researchers hadn't realised at the time was that the jamming device could have been turned into a security device for blocking the leakages that emanate from wireless communication systems.

Some researchers have suggested using robust locations scheme for the Wireless local area networks in order to control wireless activity. However their studies did not take into account malicious users, this was considered a weaknesses and the other researcher sought to put this right. In their attempt their studies fell short as it was not considered complicated enough to have covered all the areas, but was all the same considered a start on a journey into using localisation schemes in wireless local area networks (Pandey, Kim et al. 2006)

Figure 1: Modern wireless network with its risks & controls

In comparison to this other researchers have suggested the use of indoor location tracking using the RSSI readings from a single Wi-Fi access point. This was to improve on the signal reception which was a draw back in the other location tracking models. The approach used here will be of immense benefit to this study's author who will use the data collection method to collate sample variables for analyses. The study also supports the author's view that it is possible to trace-driven simulations and real life experiences to create solution models for the threats to a system (Zaruba, Huber et al. 2006).

Some of the problems facing the protocols like the IEEE 802.11 which are used for wireless networks include performance and quality of real time services due to the band-width. Currently the existing band-width which is commonly used is the 2.4GHz unlicensed industry band which is also used at home.

In order to overcome these traffic congestion threats, simulation models have been used to show that it is possible to provide a solution to the 'Threat' model. This reasoning is in part why this study is being carried out, and that is to use a simulation experiment to show that a security threat can be simulated and all the possible risks threatening the model identified in order to provide a solution. (Chen, Pang et al. 2005) In contrast to this another study suggested that the performance of a wireless network is linked to the hardware used to implement the radio and the wireless environment in which it operates. The study provides three concerns for wireless experimentation and they are ambient hardware, radio frequency hardware profiling and fading properties of the wireless channel.

The motivation for the paper was from the experience of the author's prototyping and experimenting with a wireless-layer-test bed. This will be of great benefit to this study as the paper can draw on the experiences of the researchers in developing and simulating a wireless test bed (Mandke, Daniels et al. 2007) It has been suggested that the different techniques used to protect wireless networks, stem from the standards and protocols released by the IEEE, which should be updated as and when they are released (Bhagyvati, Summers et al. 2004). The study found that the flaws which are to be updated usually stem from encryption, equipment security settings and rogue access points.

The study also found that the security vulnerabilities meant that the techniques which were in effect security controls meant stronger encryption was needed. However, the use of encryption is not the only key issue facing wireless networks and this study did not address it.

In contrast to this it was suggested that 'Threat' Models are increasingly being used to develop solutions to the existing wireless network security deficiencies (Pietro, Mancini et al. 2006). Their study developed a Threat Model to simulate the existing wireless network and then developed a 'Trust' Model with the solutions to the risks faced by the 'Threat' Model; Table 1.

The study used a simulation environment and experimented with different protocols, the researchers found that their Model could drastically decrease the computations and communications needed to establish a set of keys to unlock encrypted data. Whilst this modelling breakthrough led to many other Models being built, the study was more to do with the effectiveness of wireless networks and not security issues affecting the wireless networks.

Table 1: Threat Model tabulation for the risks to Wireless Networks

To analyse the current security threats to wireless networks: Wireless network refers to any type of computer network that is wireless, and is commonly associated with a telecommunications network whose interconnections between nodes is implemented without the use of wires, such as a computer network (a type of communications network). Wireless telecommunications networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves, for the carrier and this implementation usually takes place at the physical level or "layer" of the network.			
Dependent Variables	Data Measure of Dependent Variable	Independent Variables	Data Measure of Independent Variable
Threat Model		War driving	
		War walking	
		War chalking	
		War spying	
		War flying	

"A firm can build more effective security strategies by identifying and ranking the severity of potential threats to it's information systems efforts" (Whitman 2003). This study by a Security researcher warned of the inherent dangers facing financial organisations and what the cost to the financial industry was going to be. The study used historical cyber crime data collected from the intelligence services to show that computer security breaches had continued to increase every year, with the internet and wireless networks a frequent point of attack.

In comparison, it was suggested that the Radio Frequency Identification Prototype (RFID) be used to solve these problems and an RFID compiler was used to develop and implement and test different groups of standards or proprietary needs of a company in order to rank the severity of potential threats (Jones, Dontharaju et al. 2008). The results provided a means of hardware and software communications that facilitated the increase of prototyping RFID devices. However, the study addressed security issues in the form of power management and not external threats from unauthorised persons trying to gain access to sensitive data

4. RESULTS AND DATA ANALYSIS

The purpose of this study was to explore the rationale that governs wireless network security Figure 2, in order to do this a questionnaire study approach was used. The research approach took the form of a qualitatively designed questionnaire, in collating the methods used by management in the implementation of wireless network security within their organisations. Three stages of the research process had to be completed in order to gather the necessary data for the research.

The first was to interview the suppliers and end users of the technology used in developing wireless network security. The second was to select a representative number of companies from an electronic published database called FAME, which contains information on 3.4 million companies, 2.8 million of which are in a detailed format for companies in the UK and Ireland. The third was the administration of a Likert-type questionnaire in which respondents answered 23 unique items relevant to their job specifications (3 on IT policy) and (20 on managing the confidentiality, integrity and availability of network security and data).

Figure 2: Conceptual Map of the Evolution of wireless networks with its risks & controls

So the research follows a case study methodology on Network Security provided by the 23 small medium enterprises in England (UK) that were used. In this paper, we attempt to fill in the gap in contemporary literature based on research which explores the rationale that governs the implementation of Network Security Trust Models in small medium enterprises (SMEs) through a questionnaire study approach. In doing so, we identify the various security related perceptions held by executive and functional personnel and the degree to which these perceptions are similar.

The questionnaire was coded to represent the five key areas of the research: Software quality issues associated with (wireless location based systems); Limitations in current (wireless location based systems) models; Ethical issues in (wireless location based systems). Current security threats to wireless networks; IT governance standards for (wireless location based systems); Wireless protocols for (wireless location based systems)

The study will suggest steps that an Information Technology service may follow in order to apply a questionnaire approach to a Network Security self-assessment in a successful manner. It also provides an insight for ICT managers, directors, academia and organizations, who wish to develop an exercise in Network Security self-assessment using a questionnaire approach. It has been argued in the past that there is a lack of empirically based research to effectively analyse the security perceptions used to implement Network security within organisations; this paper presents the results of a three-stage novel framework on an empirical case study focused on 23 SMEs in England (UK).

Empirical evidence gathered from a pilot survey showed that personnel from different organisations have different perspectives towards network security. In particular, they indicate that the differences in perceptions were on areas such as the Ethics, challenges to effectively protecting the OSI Physical Layer 1 and the Quality of Service.

Table 2: Executive Level Response Chart showing respondents replies to questionnaire

Table 3: Managerial Level Response Chart showing respondents replies to questionnaire

In using the questionnaire the Network Security Model sought to identify 3 key areas which had earlier been identified by researchers as key to developing Information Security Trust Models; Sumner, M. (2009)

- To determine the risk assessment of Network security threats based upon the perceived impact of these information security threats and the perceived probability of occurrence of each of these threats.
- To determine the extent of risk mitigation based upon the perceived level of preparedness to deal with each of these Network security threats.
- To determine the extent to which the perceived probability of occurrence of information security threats and the perceived impact of Network security threats relate to the level of preparedness for dealing with these threats.

These key areas were also identified by previous research but in addition suggested that the continuous change in threats to Network Security meant that Models themselves had to be flexible

a) Executive Level Respondents (Table 2)

Information Technology Management Information (IMI):

- IT Steering / Strategy committees with minutes of meetings
- Documented IT strategy and budget (both of which have been approved)
- Regular reports for senior management team to monitor system performance

Security Awareness and Management (SAM):

- IT risk register linking IT security risks to the business objectives of the organisation (i.e. impact upon operations if realised)
- Documented security policy, which is introduced to new members of staff as part of the induction process and reminders are issued to all other members of staff (such as when there are changes)
- Processes in place to gather any security incidents are reported to the appropriate members of staff and escalated in a timely manner

b) Managerial Level Respondents (Table 3)

Implementing new Technology and emerging technology (ET):

- The organisation has representatives that participate in and attend technology forums to understand developments in technology

User Access to Systems (UAS):

- User administration processes are in place to ensure: New user set up requests are approved by an appropriate member of management
- Administrators are informed of internal transfers, so inappropriate access rights are removed
- Administrators are informed of leavers, to ensure access rights are removed in a timely manner

5. CONCLUSION AND FUTURE WORK

By using a holistic approach to understanding the development and management of protocols for wireless security and privacy locations, the study ascertained how the location of key data transmitted over the wireless network could be restricted to defined areas in order to enhance security.

It became known that human factors played a leading role in aiding these deficiencies and as such researchers have tried to address these issues by suggesting user strategies for managing security on a daily basis (Dourish, Grinter et al. 2003). It was suggested that the reason why humans played a leading role was due to the barriers raised by the security mechanisms which humans found unhelpful and as such human computer interface designers have been removing them in order to get better custom for their products.

The other findings from this research will be truly helpful in justifying why my research approach is Methodological triangulation. This is due to the research methods used to collect data. The collection of data stems from the questions asked and how the answers will be collected; some of the questions will form part of this studies survey interview and will include a) staff experience of security, b) staff attitude towards security, c) staff frustrations, d) staff pragmatism about their security needs, e) staff expectations of security as a barrier f) security as a whole: online and off line g) staff practices and security h) delegation of security i) secure actions j) holistic security management approaches k) managing identity

6. REFERENCES

- Stubblefield, A; et al. (2004) 'A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)' in *ACM Transactions on Information and System Security*, Vol. 7, No. 2, May 2004, pg 319–332.
- He, C. et al (2005) 'A Modular Correctness Proof of IEEE 802.11i and TLS' in *A formal analysis of Crypto Protocols; Proceedings of the 12th ACM conference on Computer and communications security CCS '05*, pg 2
- Xu, K. (2002) 'TCP Behaviour across Multi-hop Wireless Networks and the Wired Internet' in *Mobile Ad hoc Networks; Proceedings of the 5th ACM international workshop on Wireless mobile multimedia WOWMOM '02*, pg 41-
- Mahajan, R. (2006) 'Analyzing the MAC-level Behaviour of Wireless Networks in the Wild' in *ACM SIGCOMM Computer Communication Review*, *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '06*, 36(4) pg75-
- Gruteser, M. and Grunwald, D. (2005) 'Enhancing Location Privacy in *Wireless LAN through Disposable Interface Identifiers: a Quantitative Analysis*' *Mobile Networks and Applications*, 10(3) pg 315-325
- Kowitz, B. and Cranor, L. (2005) 'Peripheral Privacy Notifications for Wireless Networks' in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society WPES '05*. pg 90-96
- Bhagyavati et al. (2004) 'Securing Wireless Data: System Architecture Challenges' in *Proceedings of the 1st annual conference on Information security curriculum development InfoSecCD '04*; pg 82-87
- Higby, C. and Bailey, M. (2004) 'Wireless Security Patch Management System' in *Proceedings of the 5th conference on Information technology education CITC5 '04*, pg 165-168
- Hori, Y. and Sakurai, K (2006) 'Security Analysis of MIS Protocol on Wireless LAN comparison with IEEE802.11i' in *wireless mobile networks Mobility 06*, Oct. 25–27, 2006, Bangkok, Thailand; Pg1-5
- Wright, C.V. (2006) 'On Inferring Application Protocol Behaviours in Encrypted Network Traffic' *The Journal of Machine Learning Research*, 7(2006) pg 2745 - 2769

- Bhagvati, W. Summers, et al. (2004) "Wireless security techniques: an overview." *ACM*: 82-87.
- Chen, J., A. Pang, et al. (2005). "High performance wireless switch protocol for IEEE 802.11 wireless networks" *Mobile networks applications* 10: 741-751.
- Dourish, P., R. Grinter, et al. (2003) "Security in the wild: user strategies for managing security as an everyday, practical problem" *Pers Ubiquity Computers* 8: 391-401.
- Friday, A., M. et al (2003) "Network Layer Access Control for context Aware IPv6 Applications" *Wireless Networks* 9: 299-309
- Jones, A., S. Dontharaju, et al (2008) "Radio Frequency Identification Prototyping" *ACM* 13(2).
- Pietro, R., L. Mancini, et al. (2006). "Energy efficient node-to-node authentication and communication confidentiality in *wireless sensor networks*" *Wireless Networks* 12: 709-721.
- Pandey, S., B. Kim, et al. (2006) "A low cost robust localisation scheme for WLAN" *ACM*
- Mandke, K., R. Daniels, et al. (2007). "Physical concerns for cross-layer prototyping and wireless network experimentation" *ACM*: 11-18
- Whitman, M. (2003) "Enemy at the gate: Threats to Information Security" *Communications of the ACM* 46(8): 91-95.
- Wong, S. (2003). "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards" *SANS Institute*
- Xu, W., W. Trappe, et al. (2005). "The feasibility of launching and detecting jamming attacks in wireless networks" *ACM*: 46-57.
- Sumner, M. (2009) Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness IN "*Information Systems Management*", 26: 2–12 Copyright © Taylor & Francis Group, LLC
- Ijeh, A.C., Preston, D.S., Imafidon, C.O. (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/index.htm>
- DeLone, W.H., McLean, E.R. (2003), "The DeLone and McLean model of information systems success: a ten-year update", *Journal of Information Systems*, Vol. 19 pp.9-30.
- DeLone, W.H., McLean, E.R. (2004), "Measuring e-commerce success: applying the DeLone and McLean information systems success model", *International Journal of Electronic Commerce*, Vol. 9 No.1, pp.31-47.
- Ijeh, A.C., Brimicombe, A.J., Preston, D.S., Imafidon, C.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/vabilo_eng.asp?lang=eng
- Ijeh, A.C., Brimicombe, A.J., 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* University of East London United Kingdom <https://www.uel.ac.uk/icgs3/index.htm>
- 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* University of East London United Kingdom <https://www.uel.ac.uk/icgs3/index.htm>
- Ijeh, A.C., Preston, D.S., Imafidon, C.O. (2009) "Evaluating Location Based Privacy in Wireless Networks" In *Proceedings of the 4th Annual' Advances in Computing Technology Conference (AC&T)*. 27 January 2009, pp 142-150. University of East London United Kingdom <http://www.uel.ac.uk/act/index.htm>