SECURITY FRAMEWORK FOR MOBILE LEARNING ENVIRONMENTS

Shaibu Adekunle Shonola, Mike Joy

Department of Computer Science, University of Warwick (UNITED KINGDOM)

Abstract

Mobile learning is becoming popular among educators as academic technologies advance. Mobile devices used in mobile learning can potentially become vulnerable if the security aspects are neglected, thereby putting personal information of users at risk. Therefore, for mobile learning applications to work effectively as valuable tools, the security aspects must be given adequate consideration. This paper proposes a security framework for mobile learning applications which is the bedrock for designing and implementing a highly secured environment for mobile devices. The proposed framework is a generic one having capability to trap any attack or threat from any vulnerable points based on triad CIA dimensions identified in the framework. It also proposed solutions to security threats during or after development of mobile learning systems. The framework is best applied at different sub-framework levels of mobile client, server and network infrastructure vulnerability points in order to capture threats and prevent attacks that are unique to each attack route.

Keywords: m-learning, mobile learning, security, security standards, vulnerability points.

1 INTRODUCTION

Mobile learning is an emerging innovation that is being integrated into distance and e-learning programmes to deliver a complete package of virtual education [1]. The use of mobile devices in education introduces new threats to the learning environment, as they are becoming targets because of their widespread use [2]. Protecting learning content against manipulation and other users' data are inevitable [3], particularly in developing countries such as Nigeria which was ranked sixth in internet security threats and web based attack [4]. The security aspect of mobile learning is becoming increasingly important as more universities are deploying mobile technologies to complement their classroom learning delivery. The security framework for a reliable mobile learning environment is discussed in this paper.

The second section of this paper is a review of related work on mobile learning security and various frameworks. It summaries existing work on mobile learning security and related frameworks and evaluates their various recommendations. The third part discusses the architectural design of technologies used in mobile learning environments. It describes the mobile client, the three server tier (app, web and database servers) and the network infrastructure involved. The general security requirements (confidentiality, authenticity, mobile data integrity, control, availability and utility) recommended in computer security are discussed in the forth part of the paper while the three triad dimension of security (Confid entiality, Integrity and Availability (CIA)) are fully explored in a mobile learning context.

The fifth section of this paper looks at a proposed framework for a mobile learning environment. It discusses the generic holistic security framework and relates it to different threats and attacks, vulnerability points and the triad CIA dimension discussed in other sections of the paper. The sixth section of this paper is an application of the framework breaking it down into sub-frameworks of mobile client, server and network infrastructure. It highlights various threats and attacks that can penetrate each sub-framework and a technology solution to them. The paper concludes by describing the most common attack routes and directions for future work in developing a robust and highly secure mobile learning environment.

2 LITERATURE REVIEW

Conceptual frameworks for m-learning design and evaluation ranging from complex multi-level models to smaller frameworks have been proposed in the literature, the general themes among them being portability of m-learning device, learners' mobility and interaction, and control [5]. These frameworks provide the design requirements for developing m-learning applications that can be used to support classroom or distance learning [6]. There are notable works on mobile learning and security framework, some of which are examined below.

Parsons *et al.* [7] propose a conceptual design requirement for an m-learning framework based on four perspectives: generic mobile environment, learning contexts, learning experiences and learning objectives. Their framework, which was derived from many successful m-learning programmes, can be used to design learning materials for m-learning. According to them, the m-learning framework design should detail the entire process from the environmental considerations in which it will operates to the actual m-learning activities. The environment considerations basically involve close examination of mobility, user interface, use of high quality multimedia and communication support.

Nordin *et al.* [8] propose an m-learning design framework for lifelong learning, which mainly depends on the work done by Parsons *et al.* [7]. While the key elements of their models remain the same, the framework is amended to suit the purpose of the content for lifelong learning. Nordin *et al.'s* [8] m-learning framework design is also based on four elements which are: theories of learning, generic mobile environment, mobile learning context, and learning experience and objectives. However, designing content for e-learning differs from designing content for mobile learning which may be due to many physical factors such as screen size.

Another notable m-learning framework was proposed by Mohammad *et al.* [9], based on their view that m-learning is an extension of e-learning. Their framework involves adapting e-learning materials for use in mobile devices. They stated that, in doing so, some key dimensions have to be addressed and adapted. They identified the key dimensions to be learning context, users, mobile device and connectivity. Their study further analysed the context in which m-learning will be used, the users and their characteristics, as well as learning strategies. Their study covered the technical aspects of the environment in which the m-learning will operate such as cost, connectivity and speed. They also considered the mobile devices and their operating system platforms on which the devices function.

Another similar framework for m-learning based on an education component system built on three main elements was developed by Mostakhdemin-Hosseini and Mustajärvi [10] indicates that m-learning is also an extension and future of e-learning education. Their framework identifies existing e-learning platforms, wireless access point technology and mobile usability as the three key elements of the m-learning framework. Mobile usability involves determining the services of a mobile device that are used in the m-learning system. It includes the type and features of the mobile device, the mobile content design and the nature of the services. In developing a mobile learning system, wireless network infrastructures, speed, capacity and cost of services should be considered [10–11]. The existing e-learning system will influence the m-learning system being developed, but m-learning systems which are adaptive to the users and mobile devices, are more complex than the typical e-learning technologies. Instructors and learners will also influence the selection of e-learning types and distribution of services to the mobile devices.

Motiwalla [6] proposes a framework that consists of two levels, which are mobile connectivity and e-learning. While mobile connectivity focuses on the application and technology to enhance mobile content delivery, e-learning supports a set of pedagogical approaches for constructive learning and personalisation. Many other researchers state that m-learning is a combination of mobile hand held devices and e-learning and they are of the view that m-learning is an integral extension of e-learning in order to enable students to study both inside and outside the classroom [12].

However, Sharples *et al.* [13] argue that because of the uniqueness of m-learning, an e-learning framework cannot be used for m-learning materials. Parsons *et al*. [7] also share this view. Both Sharples *et al.* and Parsons *et al.* further state that the benefits and limitations of mobile devices have to be noted and addressed accordingly in designing m-learning frameworks and learning materials. In addition, the adaptation of existing e-learning frameworks and materials for use in m-learning platforms is a challenge [14]. Osang *et al.* [15] also argued that m-learning is not a mere extension of e-learning, but rather a different learning paradigm and approach. They stated that this is obvious when considering the way mobile devices are used in relation to desktop or even laptop machines for learning purposes. In fact, the differences between e-learning and m-learning are so prominent that entire different paths are followed toward information presentation, instructional design, graphic and user experience design.

Obodoeze *et al.* [16] discuss a mobile security framework for Nigeria. Their proposed framework is based on the security triad of safety, attack and privacy. It also covers the physical, data and operational safety of mobile telecommunication infrastructure. They propose 5 security frameworks for implementation by mobile companies which are security framework against attack; on GMS data confidentiality and integrity, on a corporate network, against loss of mobile equipment or phone and bombing of mobile base stations, from malicious programs and from hackers and malicious programs as a result of subscriber ignorance. Although all their proposed frameworks are suited for telecom companies in Nigeria for implementation, they cannot be easily adapted for mobile learning environments.

Ramjan [17] develops a conceptual framework of m-learning security for a university in Thailand in a hierarchical form with threats and problems at the top, followed by vulnerability points, technological solutions, CIA triad, ISO/IEC27001 and ISO/IEC17799:2005 standards and m-learning systems. However, his work was developed mainly for a Thailand University and would probably not be suitable for most African university environments.

The literature mentioned above either discusses the mobile security framework or mobile learning framework. Except the work of Ramjan [17] that discusses the conceptual framework of m-learning security in Thailand, no known conclusive work has been done on mobile learning security frameworks for developing countries in Africa. This paper will therefore, discuss the mobile learning security framework in detail starting with the general requirements needed for developing highly secure mobile learning to the proposed framework and its experimental application.

3 ARCHITECTURE

An m-learning framework normally incorporates system architecture and design learning flow. It is a systemic configuration and implementation of mobile devices for learning. The m-learning system architecture is a 3-layer design comprising of the (i) mobile device for m-learning, (ii) the m-learning servers (app, web and database) and (iii) the m-learning network infrastructure [18-20]. The m-learning mobile clients consist of different variety of mobile devices such as smartphones, tablets, PDAs, and mobile phones, and they are often programmed using different operating systems. The user interface is automatically modified to different screen sizes of the devices and connects to the servers using a Wi-Fi or WAP through a web browser. In an educational context using wireless network implementations, Wi-Fi technology is most widely used in comparison to others wireless [18, 20]. There is regular content update through synchronisation and the entire application is also updated when new features are added. The m-learning clients provide learning services such as viewing or accessing learning content and grades, downloading learning materials, having group discussion among learners and submitting assessments and feedback.

The m-learning server comprises different servers that connect the m-learning mobile devices with database servers such as the application server and web server. While the app server consists of the web portal service that handles the direct requests from WAP or Wi-Fi and it acts as a gateway between the database servers and the mobile devices, the web server accepts requests for learning content from mobile clients. The database server contains the data on learners such as their login account, enrolment details, e-portfolio and assessment grades. It also holds data on the instructors as well as the learning content [21]. Network infrastructure equipment ranges from switches and routers for Wireless Local Area Networks (WLAN) normally used within a university campus for transmitting and receiving radio signals and equipment for encrypting and decrypting educational data transmitted. Nowadays mobile broadband signals are used by mobile devices for connectivity. There are public and private Wi-Fi hotspots which can also be connected to within the institution environment or household to access m-learning servers.

4 GENERAL REQUIREMENTS FOR M-LEARNING SYSTEMS

M-learning systems need effective security technologies to ensure adequate protection from different attacks and threats. A threat is anything that has potential to cause serious harm by disrupting the operation, functioning, integrity, or availability of a network or device and it can take any form of sabotage and can be malicious, accidental, or an act of nature. On the other hand, an attack is an attempt used to exploit vulnerability to gain unauthorised access to, and make use of an learning materials and data and it is aimed to destroy, expose, alter, disable, and steal m-learning confidential information. Vulnerability is an inherent weak point in the design, development, configuration or implementation of a m-learning system or network that renders it liable to a threat, making it susceptible to information loss and downtime [22].

Several researchers have noted that privacy issues remain a key concern in m-learning environments to avoid confrontation with any security threat [23]. The basic concepts of security requirements in m-learning system to be considered in order to cope with threats are confidentiality, authenticity, integrity, control, availability and utility among others. Confidentiality is breached when important and personal information is disclosed to an unauthorised user within the m-learning environment [24] and it is also an obligation to protect other learners' personal information [25]. Confidentially is compromised when data is sniffed on a network by an intruder or when a mobile device with sensitive data or assessment grade is stolen or lost. This could possibly allow unauthorised person to access confidential information [26].

Availability ensures that important learning content should be available to students when requested. Prompt access to appropriate information, material and learning content at any time is the essence of mobile learning [24-25]. Safeguarding from attacks by keeping information protected with regards to its confidentiality and integrity is of no importance if the information is unavailable when required [26].

The integrity of data stored or accessed by mobile devices should be protected by ensuring that the data is correct and consistent, and that it cannot be created, changed or deleted by unauthorised entities. This data should be consistent throughout the whole area of its usage [24]. In the mobile technology context, data integrity also ensures that transmitted data is not intercepted, altered and modified in the process of transmission [26]. In a mobile learning environment, integrity loss can occur, for example, when a student is able to change their grade online instead of only viewing it.

Authenticity of data is the originality of content and also involves correct labelling or attribution of information which should be both genuine and original [24]. It is the process of verifying an identity given by or for an entity. In a mobile learning context, authenticity has two steps: identification, which is to present an identifier to the security system, and verification, which is to generate authentication information that corroborates the link between the identifier and the entity [27]. Mobile learners are normally required to pass through authentication steps in order to have access to learning materials.

Control concerns the physical control of the information without any need for disclosure [26]. If a mobile device is stolen, it results in a loss of control for the owner. However, it does not necessary imply a loss of confidentiality as the thief may not be able to gain access to the data due to techniques such as encryption and passwords. Data utility ensures that the data should be useful and purposeful [26]. The data that is stored and accessed by mobile devices should be fit for purpose and if after securing data by encryption and the key is lost, the data should still be confidential, controlled, integral, authentic and available but without being useful to authorised users.

All the general requirements are given consideration in order to develop a secure mobile learning platform. However, proper application of confidentiality, availability and integrity in designing mobile learning security encompass and absorb the functions of other requirements. Therefore, confidentiality, availability and integrity are regarded as the CIA triad dimension of security [17] and the proposed framework presented in this paper is based on this triad of security requirements.

5 THE PROPOSED FRAMEWORK

Our proposed framework involves identifying and safeguarding possible entry points in the client, servers and network infrastructure of an m-learning system which maybe prone to attacks from cyber hackers of wireless technology devices. The hidden weak points on lecturers' and learners' devices as well as network infrastructure need to be protected by designing a secured m-learning framework using the CIA triad dimensions: integrity, confidentiality and availability [17].

The vulnerability points in an m-learning architecture - client, server and network infrastructure - can be established by reviewing various kinds of issues, attacks and threats relating to m-learning such as illegal access to data due to device theft or loss, unauthorised penetration into a university network and using m-learning resources by unauthorised persons pretending to be real learners and lecturers in university, device and network corruption causing inconveniency to users, and attacks on the m-learning system from malicious software or viruses in mobile applications and devices of students, lecturers and on the network [28].

In order to overcome these issues, adequate security policy to block or secure the vulnerability points of m-learning system in accordance with the CIA triad dimensions based on ISO/IEC27001 and ISO/IEC17799:2005 standards can be employed [29]. The security policy provides mobile device and network risk management that is associated with scope, term and definition of use of devices, and the structure of risk assessment and management.

Identifying and understanding the security weak points at mobile client, server and network levels are very important in overall design strategy for a secured m-learning framework [17]. Once a threat or attack and its possible vulnerability points are known, providing possible solutions based on the CIA triad dimensions is feasible.

Fig. 1 is the proposed mobile learning framework presented in this paper. It is a generic framework having three sections: the threats and attacks, mobile learning environments and possible solutions. The mobile learning environment is subdivided into vulnerability points and the CIA triad security requirements. The vulnerability points or attack routes are the mobile clients, servers and network infrastructure described in section 3 under architecture. The triad CIA security requirements are Confidentiality, Integrity and Availability, discussed under the general security requirement. The mobile learning framework can detect any threat and deter any attack if the triad CIA security measures are properly implemented in the design and development of mobile clients, servers and network technology of the mobile learning environment. However, if hackers are able to penetrate the learning using sophisticated and latest hacking techniques without being detected, a further review of the CIA security requirement should recommend a possible solution. Thus, the generic framework should detect any possible threat and attack and offers possible solution based on the vulnerability entry point and triad CIA security measures.

Threats and attacks can penetrate the mobile learning environment through the mobile device or client, the server or the network equipment as they are indicated to be the vulnerability points or attack routes into the system. A threat can spread from one vulnerability point to another and penetrate all the other mobile learning systems as the devices are connected to one another. Depending on the purpose of the attack and the inbuilt security measure, a threat can be propagated among the devices once it has entered through a vulnerability point and cause multiple damage. In a mobile learning context, the database server may be a major target since all students' personal information, assessment, grades and feedback are centrally stored in it while the mobile device may be a target if the purpose is to have unauthorised access to learning content downloaded in it.

Similarly, once a threat penetrates successfully, it can affect one dimension of the triad CIA or all. Threats that affect integrity can also affect confidentiality or availability or both. Therefore, in tackling any threat or attack, adequate consideration should be given to the availability, integrity and confidentiality in order to achieve a meaning and lasting solution. More importantly, utmost consideration should be directed at the triad CIA requirements at the onset during design, development, implementation and deployment of a new mobile learning environment.

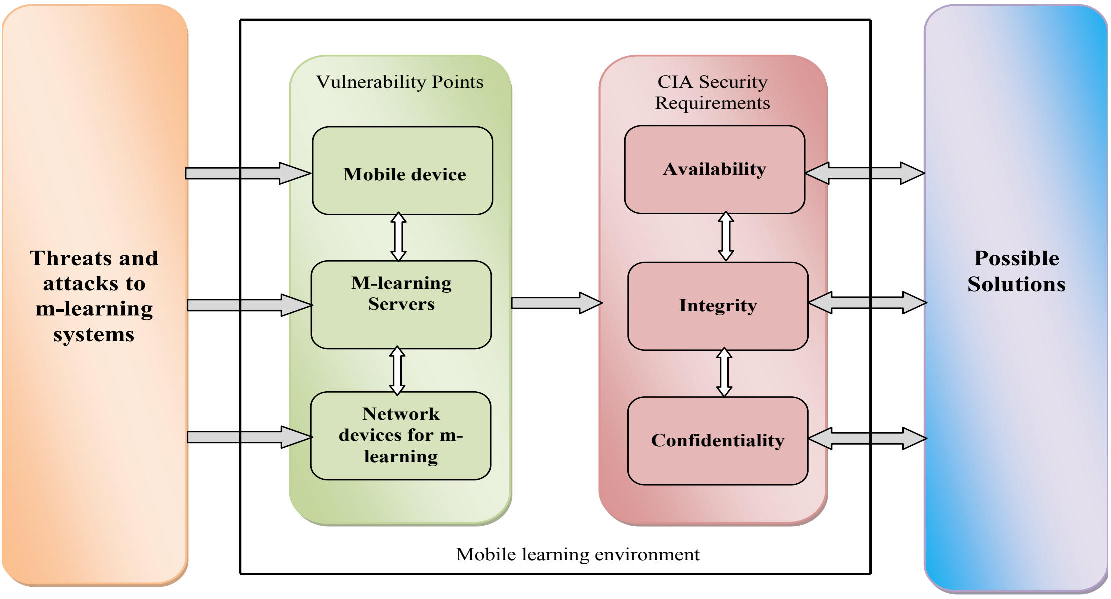
Threats and attacks to m-learning systems
Vulnerability Points
Mobile device
M-learning Servers
Network devices for m-learning
CIA Security Requirements
Availability
Integrity
Confidentiality
Mobile learning environment
Possible Solutions

Fig 1: Proposed m-learning security framework

6 APPLICATION OF THE FRAMEWORK

The proposed framework can be applied at each vulnerability point. The framework is subdivided into three sub-frameworks based on their vulnerability points - mobile clients, server and network infrastructure sub-framework - in order to determine threats and attacks that are peculiar to each weak point, how the triad CIA dimensions affected are handled, and possible solutions to tackle each and every threat and attack.

6.1 Mobile Client Sub-framework

This is a subset of the generic mobile learning framework in fig. 1. It is designed and built to detect, prevent and give a solution to any attack or threat to mobile devices. Fig. 2 shows the mobile client sub-framework, featuring the threat/attacks, vulnerability points, security requirements and possible solutions. If a mobile device is lost or stolen, the CIA requirement affected is the availability as the device cannot be available for legitimate use. Regular online data backup can make another copy of data available for immediate use. The location of the mobile device can be tracked and found if lost or reported to security personnel if stolen. Remote wipe can be used for factory reset on the device to avoid confidential data being accessed by unauthorised personnel. Malicious programs attacking mobile devices affect the triad CIA security requirements.

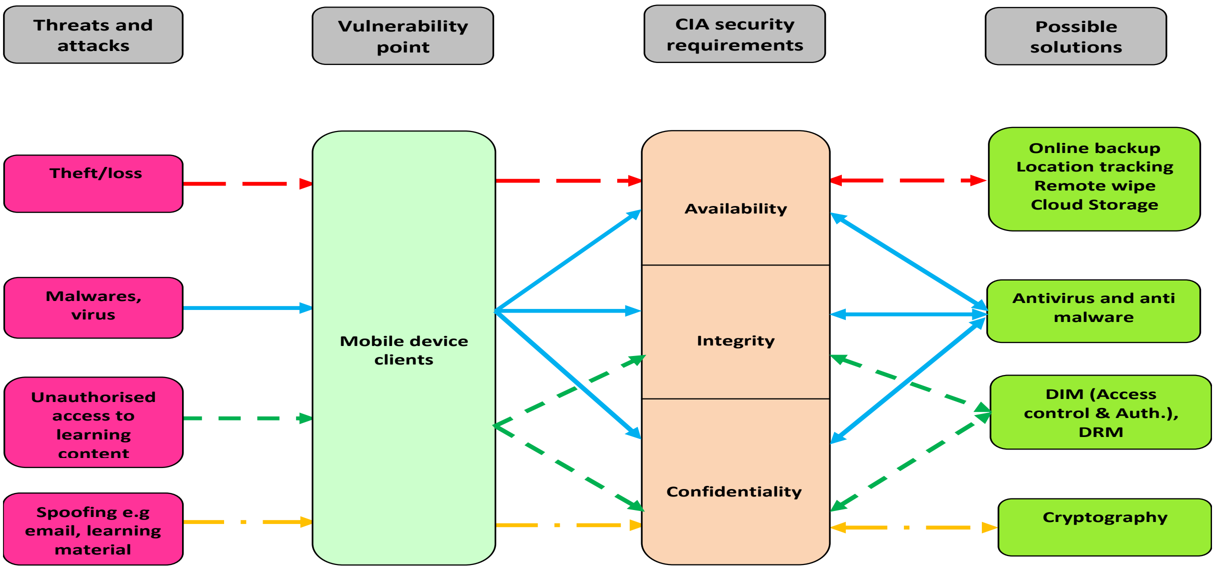

Fig 2: Mobile client security sub-framework

6.2 Server Sub-framework

The server sub-framework is developed to protect the m-learning host systems from various threats and attacks. Physical attack affects availability and it is possible where there is no physical security policy in place, and can be minimised and deterred by access control and CCTV cameras. Activities of hackers and malicious programs target poorly designed servers and affect the availability, integrity and confidentiality. Putting in place the triad CIA requirements through regular patch updates and installing antivirus/malware can deter threats and attack. Fig. 3 is a server sub-framework detailing possible threats and attacks, CIA requirements and possible solutions to them.

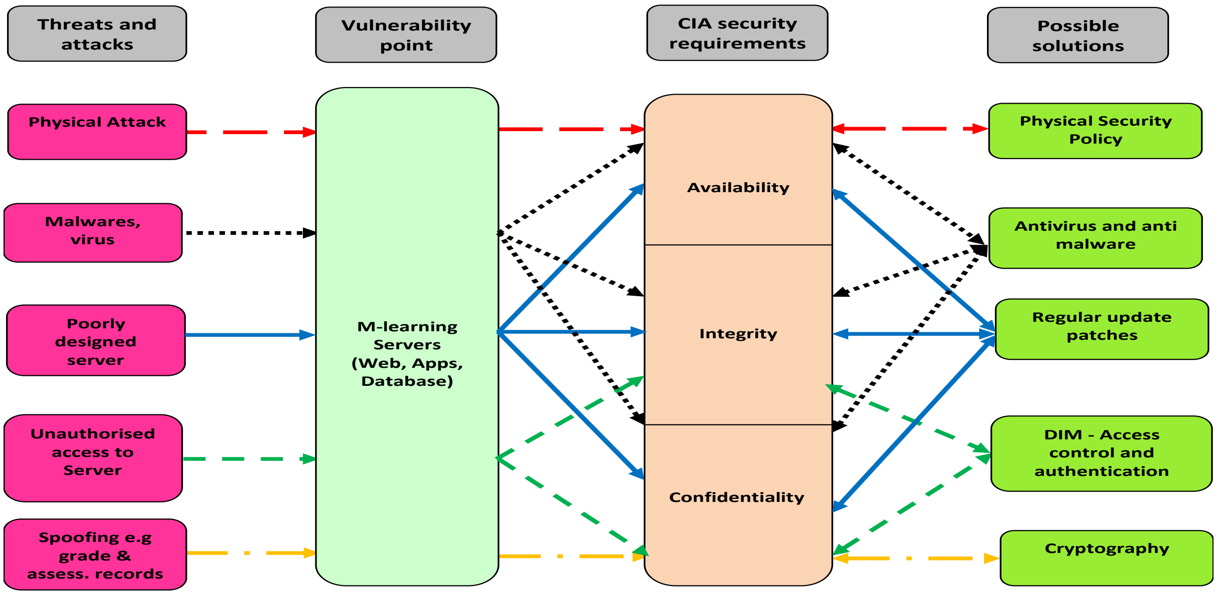

Fig 3: Server level security sub-framework

6.3 Network Infrastructure Sub-framework

Aside from a physical attack that affects availability and can be prevented with adequate physical security policy, unscheduled down time/ disruption in form of power outage is a major network infrastructure threat. This is common in many developing countries where there are daily power cuts in most cities. Physical attacks on network infrastructure on campus are also common, for example during student riots in some universities in developing countries such as Nigeria. Unscheduled downtime or disruption affects availability requirement and can be overcome by uninterruptible power supply and scheduled maintenance policy. Fig. 4 is a network infrastructure sub-framework detailing possible threats and attacks, CIA requirements and possible solutions to them.

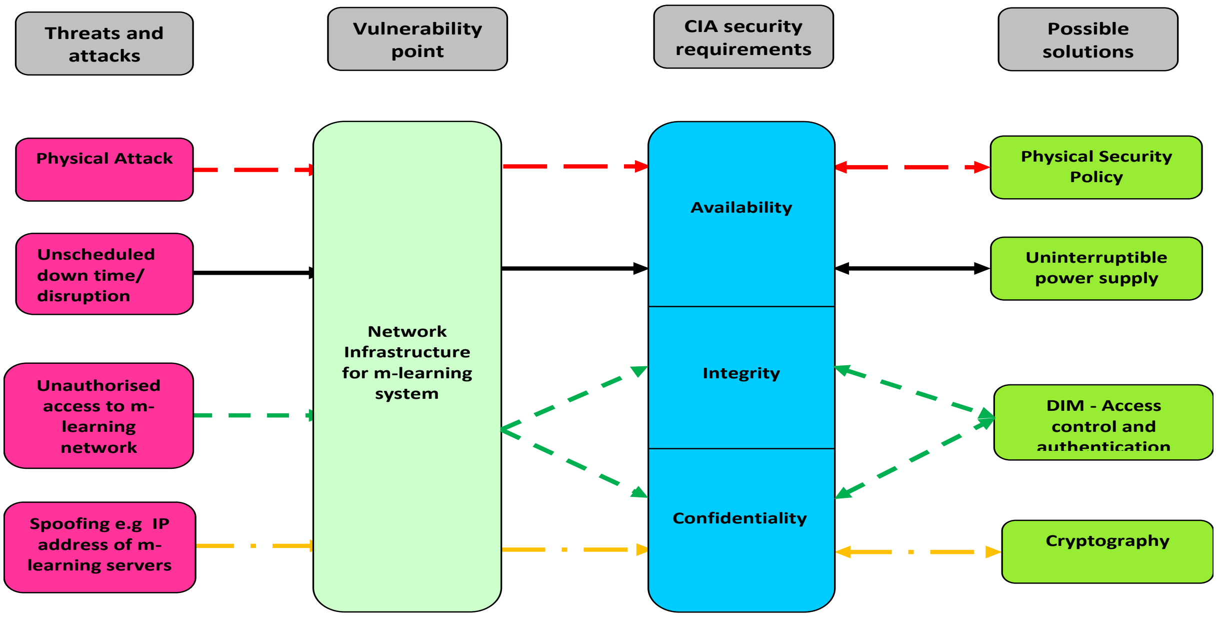
Threats and attacks
Vulnerability point
CIA security requirements
Possible solutions
Physical Attack
Unscheduled down time/ disruption
Unauthorised access to m-learning network
Spoofing e.g IP address of m-learning servers
Network Infrastructure for m-learning system
Availability
Integrity
Confidentiality
Physical Security Policy
Uninterruptible power supply
DIM - Access control and authentication
Cryptography

Fig 4: Network Infrastructure sub-frame

The threats that affect the three sub-frameworks are unauthorised access and spoofing. While unauthorised access targets integrity and confidentiality of the security dimension, spoofing affects mainly the confidentiality. Access control and authentication possible solution to unauthorised access, cryptography can handle threats from spoofing activities.

The framework and the sub-frameworks were further examined and evaluated during a study on mobile learning security in four universities in Nigeria. The feedback from the survey shows that 9 out of ten participants agreed that security issues around confidentiality, integrity and availability are major concerns in implementing and deploying mobile learning successfully in Nigeria education institutions. A detailed analysis of the study is reported elsewhere [30].

7 CONCLUSION AND FUTURE DIRECTIONS

This paper discussed a novel mobile learning security framework that can be used as a foundation for designing and implementing a highly secured mobile learning environment. The framework and sub-frameworks are based on literature of good practice, ISO/IEC27001 and ISO/IEC17799:2005 standards and the framework proposed by Obodoeze *et. al* [16]. However, certain adaptations have been made to the framework to make it suitable for a learning environment. While Obodoeze et al.'s [16] research work is suited for telecom operators in Nigeria and their framework is based on the security triad of safety, attack and privacy, the framework proposed in this paper is based on the CIA triad and is focussed on higher education institutions. Our proposed framework is in line with the research done by Ramjan [17] and El-Gamil and Badawy [18] but provides a broader view by taking into account up to date information, modern mobile devices and latest development technologies in the design of the framework.

The application and evaluation of the proposed framework and sub-frameworks in a study conducted recently in Nigeria Higher education institutions on mobile learning security show that threats and attacks are more predominant on the mobile client devices than on the server and network infrastructure [31]. Therefore, future efforts on security framework should be directed to having extremely secured mobile client devices.

REFERENCES

[1] Ozuorcun N,C and Tabak, F. (2012). 'Is m-learning versus E-learning or are they supporting each other'. 4th WORLD CONFERENCE ON EDUCATIONAL SCIENCES (WCES-2012) 02-05 February 2012 Barcelona, Spain. pp. 299-305

[2] Howell, M., Love, S. and Turner, M. (2008). 'User characteristics and performance with automated mobile phone systems'. International Journal of Mobile Communications. Vol. 6, no. 1, pp. 1-15.

[3] Luminita, C. D.C. and Magdalena, C.I.N (2012). 'E-learning Security Vulnerabilities'. 4th WORLD CONFERENCE ON EDUCATIONAL SCIENCES (WCES-2012) 02-05 February 2012 Barcelona, Spain.pp. 2297–2301

[4] Chidiogo, E (2013). Nigeria ranked sixth in Internet security threat. [Online] Available from http://telegraphng.com/2013/06/nigeria-ranked-sixth-in-internet-security-threat/ [Accessed on 10-January-2014]

[5] Kearney, M., Schuck, S., Burden, K. and Aubusson, P.(2012). 'Viewing mobile learning from a pedagogical perspective'. Research in Learning Technology. Vol.20, no.1, pp. 1-17

[6] Motiwalla, L.F (2007). 'Mobile Learning: A framework and evaluation'. Computers & Education. Vol. 49 no. 3, pp. 581-596

[7] Parsons, D., Ruy, H. and Cranshaw, M (2007). 'A Design Requirements Framework for Mobile Learning Environments'. A Journal of Computers, vol. 2, no. 4, pp. 1-8.

[8] Nordin, N., Embi, M.A. and Yunus, M.M. (2010). 'Mobile Learning Framework for Lifelong Learning. International Conference on Learner Diversity 2010'. Procedia - Social and Behavioral Sciences. Vol. 7, no.10, pp. 130-138.

[9] Mohammad, H., Mohammad A., Hamdan, Z., and AboAli, A. (2007). 'A Framework for Mobile Learning Content Design'. A Paper presented in ICT-Learn 2007 Sixth International Internet Education Conference and Exhibition Cairo

[10] Mostakhdemin-Hosseini. A and Mustajärvi, J (2003). 'Framework for mobile learning system based on education component'. Proceedings of the International conference on Theory and Application of Mathematics and Informatics – ICTAMI 2003, Alba Iulia. pp. 191-196

[11] Udanor, C.N. and Nwodoh,A.T (2010). 'A Review of M-learning Models'. Indian Journal of Computer Science and Engineering. Vol.1, no. 4, pp. 426-436.

[12] Sitthiworachart, J. and Joy, M.S. (2008). 'Is Mobile Learning a Substitute for Electronic Learning?' In proceeding of: IADIS International Conference e-Learning 2008, Amsterdam. pp. 451 – 458

[13] Sharples, M., Taylor, J. and Vavoula, G. (2005) 'Towards a Theory of Mobile Learning'. In Proceedings of MLearn Conference 2005. [Online] Available from http://www.compassproject.net/sadhana/teaching/readings/sharplesmobile.pdf [accessed 08-July- 2013].

[14] Fayolle, J., Gravier, C., Ates, M and Lardon, J (2009). 'Remote Laboratories Framework: Focus on Reusability and Security in M-learning Situations'. International Journal of Online Engineering iJOE vol.5, no. 3, pp. 19-24.

[15] Osang,B.F., Ngole, J. and Tsuma, C .(2013). 'Prospects and Challenges of Mobile Learning Implementation in Nigeria: Case Study National Open University of Nigeria (noun)'. A paper presented at International Conference on ICT for Africa 2013, February 20 -23, Harare, Zimbabwe

[16] Obodoeze, F.C., Okoye, F.A., Mba, C.N., Asogwa, S.C. and Ozioko., F.E (2013). 'A Holistic Mobile Security Framework for Nigeria'. International Journal of Innovative Technology an Exploring Engineering (IJITEE), vol. 2, no. 3, pp.1-11

[17] Ramjan, S (2010). 'The conceptual framework of mLearning security for university in Thailand'. The Seventh International Conference on eLearning for Knowledge-Based Society, 16-17 December 2010, Bangkok, Thailand.

[18] El-Gamil, K and Badawy, O.M (2010) 'M-learning Framework for University Students'. International Conference on Computer Theory and Applications. 23-25 October 2010, Alexandria, Egypt

[19] Chris, G.S., Grebla, H. and Stanca, L (2009) 'Mobile Learning Platform for E-Learning'. International Journal of Interactive Mobile Technologies (iJIM). vol. 3, no. 3 pp. 17-20

[20] El-Sofany, H.F and El-Seoud, S.A. (2009). 'Towards the Development of an M-learning System: A New Stage to Enhance Higher Education'. International Journal of Interactive Mobile Technology (iJIM), vol.3, no. 3, pp. 4-9

[21] Basaeed, E.I., Berri, J., Zemerly, M.J. and Benlamri, R (2009) 'Web-based Context-Aware M-learning Architecture'. International Journal of Interactive Mobile Technology (iJIM). Vol.1, no.1, pp.5-10

[22] Gregory, P (2009). CISSP Guide to Security Essentials. Cengage Learning Inc. Boston.

[23] Freeman, L and Urbaczewski, A (2005). 'Why do people hate spyware?' Communications of the ACM, vol. 48, no. 8, pp. 50-53.

[24] Kabay, M.E (2007) Security for telecommuters. [Online] Available at http://www.securitytechnet.com/resource/rsc-center/vendor-wp/trusecure/telecommuters.pdf 2007. [Accessed on 02-August-2012]

[25] Anderson, R (2008) Security Engineering: A Guide to Building Dependable Distributed Systems. (2nd Edition). Wiley Computer Publishing. New York

[26] Bishop M. (2003) Computer Security: Art and Science. Addison-Wesley Publishing Company. Boston

[27] Leung, A., Sheng, Y. and Cruickshank, H (2007). 'The security challenges for mobile ubiquitous services'. Information Security Technical Report, vol. 12, no.3, pp. 162 – 171.

[28] Ghorbanzadeh, P., Shaddeli, A., Malekzadeh, R and Jannbakhsh, Z (2010) 'A Survey of Mobile Database Security Threats and Solution for IT'. 3rd International Conference on Information Sciences and Interaction Sciences (ICIS), 23-25 June 2010, Chengdu, China. pp. 676 - 682

[29] Meehinkong, T., Praneetpolgrang, P. and Mekhabunchakij, K (2009) ‘The Analysis and Evaluation of Security Readiness in ICT Infrastructure for Supporting e-Learning in Institute of Physical Education’. The Sixth International Conference on eLearning for Knowledge-Based Society16-17 December 2009, Bangkok, Thailand

[30] Shonola, S.A and Joy, M.S (2014), ‘Mobile learning security issues from lecturers’ perspectives (Nigerian Universities Case Study)’. *6th International Conference on Education and New Learning Technologies, 7-9 July, 2014, Barcelona, Spain.* pp. 7081-7088

[31] Shonola, S.A and Joy, M.S. (2014). ‘Investigating Attack Vectors in M-learning Systems in Nigerian Universities’, International Conference on Interactive Mobile Communication Technologies and Learning (IMCL), *13-14 November 2014, Thessaloniki, Greece*