

# The Conceptual Framework of mLearning Security for University in Thailand

**Sarawut Ramjan**

Department of e-Commerce Management,  
School of Business Administration,  
North-Chiang Mai University, Thailand  
sarawutr@northcm.ac.th

**Abstract**— At present, university in global and Thailand adopt mobile technology for support an education that call mLearning. Nevertheless, there are vulnerability points; client, server and network communication which could be bombarded from variously threat and problem. Therefore, this paper reviews to concerning issues in mLearning security of world wide country with Thailand in order to design the mLearning security conceptual framework for university in Thailand under C.I.A. triad dimension; integrity , confidentiality and availability that involving to ISO/IEC27001 and ISO/IEC17799:2005 standard . This framework security is decency for Thai university who provide network, application and policy for mLearning system. Moreover, this idea can be useable to prototype for further analysis model later.

**Keywords**— mLearning, mLearning security, risk management, security standard,

## I. INTRODUCTION

Nowadays, universities in global be effort to driving learning and teaching via mLearning concepts of anytime, particularly and anyplace, mLearning enhances communication of group activity for virtual class superintendence. [12] Accordingly, Thai university alert to improving an efficiency of class room management by mLearning that consists of lecturer and student tool and network infrastructure in

order to support communication party. However, mLearning infrastructure is hidden by vulnerability points; client, sever and network communication which can be harmed from cyber problem on wireless communication.

Mode of practice is review to mLearning concerning issues and technological solutions in university of each country for comparison with Thailand that relate with C.I.A. triad dimension; integrity, confidentiality and availability.

Concerning issues and technological solutions which are discovered and divided by copious of view points which is adopted for inventing the conceptual framework of mLearning security in order to displaying the security practical guideline for Thai university who developed and designed mLearning infrastructure on top level management beneath the ISO/IEC27001 and ISO/IEC17799:2005 characteristic.

## II. LITERATURE REVIEW

By the reason that university have concern and require mLearning technology for reinforce learning management. But, security is challenging for mLearning system which faces to threat and risk on Wi-Fi channel. For concentrated concerning to effect of vulnerability points in mLearning system; client, server and network communication, this review can be displayed to various kinds of problem as following [8]:

- Access to data because of device theft or loss. Student and lecture can not take activity or access to data over network communication.
- Unauthorized penetration into corporate network and application is an importance problem. If other peoples who not have authority for employ resources on mLearning infrastructure can access to mobility system, they have ability to use all feature of mLearning system as same as real student and lecturer in university.
- Device corruption is inconvenience in general university. Because IT infrastructure is prepared for all student and lecturer in university who have liberty and right to appreciate directly resources. Therefore, they should be controlled about the application and device access ability and should be limited in download bandwidth deployment.
- The last is malicious software or viruses on mobile devices. These are common threat and problem which break through an internet and computer technology. Accordingly, mLearning system can be tackled from malicious software or viruses in mobile application and device of student, lecturer and network communication.

In order to overcome these problems, Thai university drive to reforming network infrastructure under ISO/IEC27001 for enhances mLearning service security

according to C.I.A. big three of information security. ISO/IEC27001 is standard of organization, which provides network risk management that is associates to scope, term and definition, structure of risk assessing and management. In additional, they apply ISO/IEC17799:2005 which according to ISO/ICE2007 for practical direction to conspire a security system in essence of security policy, organization information security, asset management, human resources security, physical and environmental security communication and operation management, access control, information acquisition and development and maintenance, system information security incident management, business continuity management and compliance.

Thai university necessary to employ ISO/IEC27001 and ISO/IEC17799:2005 standard for mLearning infrastructure platform under C.I.A. triad characteristic. [11]

### III. EXPERIENCES COUNTRY AND COMPARATIVE THE TREND OF MLEARNING SECURITY

This investigating informs to blocking which effect to vulnerability point of mLearning system that insure against dangers from technological solution under C.I.A. triad dimension of university in worldwide country for comparison with Thai university as table below:

**TABLE 1**  
MLEARNING CONCERNING ISSUE AND TECHNOLOGICAL SOLUTION IN DIMENSION OF VUNERABLE POINTS AND C.I.A. TRIAD IN WORLDWIDE COUNTRY WITH THAIALND.

Country	Three key of vulnerability points	C.I.A. triad dimensions	Concerning Issue	mLearning Technological solution
Thailand ([9], [4])	Client	Availability	device theft or loss	Spare battery
			Malicious software	Mobile antivirus and spyware
		Confidentiality	Unauthorized access	Authentication
			Spoofing	Cryptography
			Malicious software	Mobile antivirus and spyware
		Integrity	Malicious software	Mobile antivirus and spyware
	Unauthorized access		Authentication	
		Availability	Physical attack	Security policy
			Poorly designed server	Patches update

	Server	Confidentiality	Malicious software	Antivirus and spyware
			Unauthorized access	Authentication
			Spoofing	Cryptography
		Integrity	Malicious software	Mobile antivirus and spyware
			Poorly designed server	Patches update
			Malicious software	Mobile antivirus and spyware
	network	Availability	Unauthorized access	Authentication
			Spoofing	Cryptography
		Confidentiality	Unauthorized access	Authentication
			Spoofing	Cryptography
Iran [7]	Client	Availability	Malicious software	Mobile antivirus and spyware
			device theft or loss	Spare battery
		Confidentiality	Unauthorized access	Authentication
			Fishing	Mobile token server
			Spoofing	Cryptography
			Malicious software	Mobile antivirus and spyware
	Integrity	Malicious software	Mobile antivirus and spyware	
		Unauthorized access	Authentication	
	Server	Availability	DDos	DNS server
			Malicious software	Antivirus and spyware
		Confidentiality	Unauthorized access	Authentication
			Spoofing	Cryptography
			Malicious software	Mobile antivirus and spyware
		Integrity	Poorly designed server	Patches update
	Malicious software		Mobile antivirus and spyware	
	network	Availability	Unauthorized access	Authentication
			DDos	DNS server
		Confidentiality	Unauthorized access	Authentication
			Spoofing	Cryptography
	South Africa [1]	Client	Availability	device theft or loss
Server		Availability	device theft or loss	Cloud computing
			DDos	DNS server
network		Availability	device theft or loss	Uninterruptible power supply
		Confidentiality	Poorly designed network communication	Risk management
USA. [4]	Client	Availability	Malicious software	Mobile antivirus and spyware
		Confidentiality	Fishing	Mobile token server
			Malicious software	Mobile antivirus and spyware
	Integrity	Malicious software	Mobile antivirus and spyware	
	Server	Availability	device theft or loss	Cloud computing
			Malicious software	Antivirus and spyware
		Confidentiality	Malicious software	Mobile antivirus and spyware
	network	Integrity	Malicious software	Mobile antivirus and spyware
Availability			device theft or loss	Uninterruptible power supply
UK [5]	Client	Confidentiality	Spoofing	Cryptography
		Integrity	Unauthorized access	Authentication
	Server	Confidentiality	Unauthorized access	Authentication
			Spoofing	Cryptography
	network	Integrity	Unauthorized access	Authentication
Romania [2]	Client	Availability	Malicious software	Mobile antivirus and spyware
		Confidentiality	Unauthorized access	Authentication
			Fishing	Mobile token server

		Integrity	Spoofing	Cryptography	
			Malicious software	Mobile antivirus and spyware	
		Malicious software	Mobile antivirus and spyware		
		Unauthorized access	Authentication		
	Server	Availability	Confidentiality	DDos	DNS server
				Malicious software	Antivirus and spyware
		Unauthorized access	Authentication		
		Spoofing	Cryptography		
		Malicious software	Mobile antivirus and spyware		
		Malicious software	Mobile antivirus and spyware		
	Integrity	Unauthorized access	Authentication		
		Unauthorized access	Authentication		
network	Confidentiality	Unauthorized access	Authentication		
	Integrity	Spoofing	Cryptography		
South Korea [10]	Client	Availability	device theft or loss	Spare battery	
		Integrity	Malicious software	Mobile antivirus and spyware	
	Server	Availability	Unauthorized access	Authentication	
		Integrity	device theft or loss	Cloud computing	
	network	Availability	Unauthorized access	Authentication	
		Confidentiality	device theft or loss	Uninterruptible power supply	
		Integrity	Unauthorized access	Authentication	
		Integrity	Spoofing	Cryptography	
	Greece [3]	Client	Availability	Unauthorized access	Authentication
			Confidentiality	Fishing	Mobile token server
Spoofing				Cryptography	
Integrity			Unauthorized access	Authentication	
Server		Availability	Unauthorized access	Authentication	
		Confidentiality	device theft or loss	Cloud computing	
			Spoofing	Cryptography	
network		Integrity	Unauthorized access	Authentication	
		Availability	Unauthorized access	Authentication	
		Confidentiality	device theft or loss	Uninterruptible power supply	
		Integrity	Unauthorized access	Authentication	

From harmonize above, this comparison show connecting of mLearning problem and solution that covers by C.I.A. triad and vulnerable points of mLearning in experience country irrespective of Iran, Greece, South Korea, UK, USA., Romania, South Africa, Thailand. They confront with similar to threat and problem trend that overlap to dimensions of availability, confidentiality and integrity such as malicious software mobile, unauthorized access and access to data because of device theft or loss. In technological solution view point, there are preserve way that resemble

direction such as authentication, uninterruptible power supply and mobile antivirus and spyware in client, server and communication network on mLearning system.

In order to guideline specifically in mLearning security providing, this section is compiled current issues into summarize contents which are proposed within ISO/IEC27001 and ISO/IEC17799:2005 standard view point of mLearning security development. For demonstrated, Thai and world wide university realize that security is significant key for virtual class management

that depends on mLearning system. Therefore, they are determined to defining security framework that is applied for mLearning system in university. In order to definition about security guideline that suitable for mLearning system, they work considering factor as domains below:

#### **A. Security policy**

All over the world universities are congested to unauthorized access that is prominent problem. Because, internet activity such as grad registration or examination necessary to observe by lecturer or student who have opposite accessing authorization to mLearning system. Therefore, security policy can employed for controlling, monitoring and directing people who have divergence duty or utilizing possibility for mLearning system in work quality of security awareness responsibility.

#### **B. Organization information security**

University is organization which necessary to creating about creditable and trusting into interest party on sector of information security that concerning to school-record and personal data that manipulate to long life of student. So, strongly information security should be installed in university in world wide country with Thailand for appointing the creditable of data exchange between three key of vulnerability point and take care for weak feature and device from internet barrier.

#### **C. Asset management**

Evaluation is employed for asset type classifying in order to finding vulnerability point and considering about level of risk. However, university asset in world wide country with Thailand have complicating of people who apply common data together. Thus, this process can appropriately filter each asset with loss that is possible before providing a security infrastructure in each weak point of mLearning system.

#### **D. Human resources security**

Big problem is not cyber problem but it is cultural organization. Since, mLearning security must be converted from traditional

performing into modern practice that suitable for new process working of mobile learning in university. However, security standard in human resources have to be drive in order to propose rule or procedure for people who have difference authorization and security level awareness in each duty on mobile learning infrastructure.

#### **F. Physical and environmental security communication and operation management**

Operation management should be developed concerning to physical technology that is support to communication on wireless environment in each layer of feasibility, finding, analysis, design, implement and maintaining in each university.

#### **G. Access control**

Among of difference authorization, mLearning security system should provide about system and data access capacity in difference people who can direct to resources of mLearning system. Therefore, university can push forward the policy regarding to accessible authority mLearning system.

#### **H. Information acquisition and development and maintenance**

Future information is one in all section that should be organized for improving to goodness planning. In similar to mLearning security system, it is unit that really necessary to be planned and developed about information which is adopted in each security dimension in future for support security performance. In additional, information maintenance is importance process for monitoring an operation in each phase of information management.

#### **I. System information security incident management**

mLearning should be provided about security standard which can cope with new threat and problem trend. In specify, mLearning team should prepare for incident management which involve by asset value evaluation, vulnerability point, threat and problem, potential loss, technological solution, policy and security control in order to protect mLearning system from unexpected event.

**J. Business continuity management and compliance**

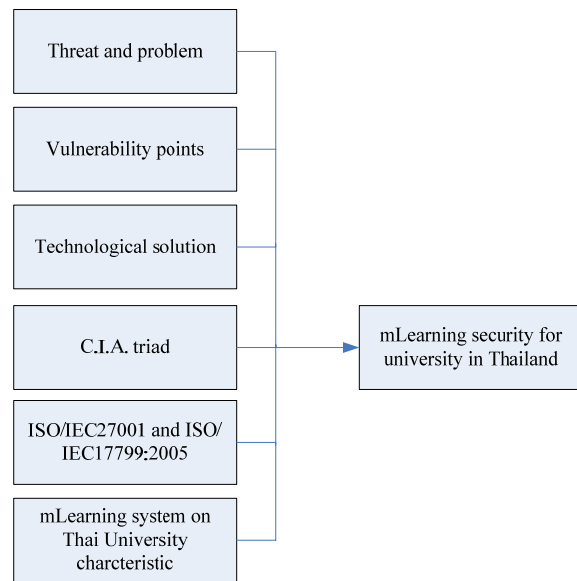
Thai and world wide university confront with this obstruct problem. One solution is the business continuity management and compliance conspire way. This method is guideline for transfix standard of security that up to date by trend of technology and future industry standard. Moreover, it is decency to university for develop mLearning security system that be proper for each defect on wireless channel.

To put in briefly, mLearning in world wide and Thai university face danger experience associating to cyber and physical damage that affect to vulnerable points; client, server and communication network in mLearning system. They are diligent to protecting this system by technological solution in according to C.I.A triad; availability, confidentiality and integrity. Hence, they think over in part of asset value estimated and forecast for potential waste in each vulnerability point in order to appraise the level of risk in each point for define security framework in their mLearning system. Furthermore, they prepare technological solution for reducing risk level and design a policy and procedure for directing and monitoring to people; lecturer, student and network technician who have difference characteristic employment for mLearning system. This standard cover to security control that is organized for check to security performance of technological solution and procedure, this overall checking is adopted for transforming into each flexible phase of security evaluation and management beneath ISO/IEC27001 and ISO/IEC17799:2005 standard.

**IV. CONCEPTUAL FRAMEWORK**

From review article about current issues and technology of mLearning security in university of worldwide country for comparison with Thailand in dimension of vulnerability point in mLearning system and C.I.A. triad that is including to

ISO/IEC27001 and ISO/IEC17799:2005 standard, this report be engross in summarizing popular issues and theory review for supporting and driving the mLearning security conceptual framework that is illustrated and represented to decency of Thai university in order to push on research and rectify the mLearning security infrastructure that can be proper with learning management system which surround to each Thai university as figure below:



**Fig. 1** The mLearning security conceptual framework for university in Thailand

From figure above, it is conceptual framework for mLearning security of Thai university. There propose to theoretical scope regarding to threat and problem which effect into vulnerability points, technological solution, C.I.A. triad, ISO/IEC27001 and ISO/IEC17799:2005 standard and mLearning system on Thai university characteristic in order to observe activity concerning to best practical guideline of mLearning security system that according to characteristic of each IT university environment in Thailand. Moreover, this framework can be useable to further study for researcher who reaches the arm to near by mLearning security main point later.

## V. CONCLUSION

There is harmonizing to concerning issues which effect to vulnerable points of mLearning system in Thai university. One solution is review literature regarding to threat and problem and technological solution that touching to set of C.I.A. triad big three dimensions on world wide university for comparison with university of Thailand in point of client, server and network communication. Moreover, this finding includes with ISO/IEC27001 and ISO/IEC17799:2005 standard in order to evaluated level of risk in each asset which have loss tendency fitting in technological solution on mLearning system border. Therefore, this document is determined to representing to gathering dimension of up-to-date event that corresponding with idea coherency.

From moment above, the conceptual framework of mLearning security for Thai university is illustrated for indicating to companionway of analysis and design about mLearning security guideline for Thai university who encounter with danger on mLearning complexion. On the other expect, this framework is path example for further analysis model that codify and analyze for similar advantage with this framework.

In order to profoundly further study, this document suggest that mLearning security can approach to dimension of law/act which is useable for preventing to client, server and network communication in view point of internet activity repudiation. On the next review, researcher can find and analysis to security issue that employ law/act for solving a problem or protecting in vulnerable point of mLearning system on communication channel for summarizing and proposing to mLearning security system that support to variety of security dimension later.

## REFERENCES

- [1] Andrea Barker, Greig Krull and Brenda Mallinson. "A Proposed Theoretical Model for M-Learning Adoption in Developing Countries". 4th World Conference Proceedings of mlearning, 2005.
- [2] Catalin Boja, Lorena Batagan, Mihai Doninea and Alin Zamfiroiu. "Secure Bluetooth Service in an M-Learning Environment". The 9<sup>th</sup> WSEAS International Conference on Software Engineering, Parallel and Distributed Systems, 2010.
- [3] Charalampos Karagiannidis, Adamantios Koumpis and George Lekakos. "m-Learning and m-Commerce in Pervasive Environments". Proceedings of the 4th World Conference on mLearning, 2005.
- [4] Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn and Farnam Jahanian. "Virtualized In-Cloud Security Services for Mobile Devices". International Conference On Mobile Systems, Applications And Services, 2008.
- [5] Kuldeep Nagi. "Solving Ethical Issues in eLearning". Third International Conference on eLearning for Knowledge-Based Society, 2006.
- [6] Lirong He, Lisha He, Ian Rogers. "new security protocol for M-Learning". IADATE-2005 International Conference on Education, 2005.
- [7] Mahdi Seify. "A Methodology for Mobile Network Security Risk Management". Sixth International Conference on Information Technology: New Generations, 2009.
- [8] P. Ghorbanzadeh, A. Shaddeli, R. Malekzadeh and Z. Jannbakhsh. "A Survey of Mobile Database Security Threats and Solution for IT". 3rd International Conference on Information Sciences and Interaction Sciences (ICIS), 2010.
- [9] Sang Tae Kim, Asif Iqbal, Byoung-Ju Yun, Jonghun Baek, and Hyun Deok Kim. "Mobile eLearning System Employing a Jini-Agent". Fourth International Conference on eLearning for Knowledge-Based Society, 2007.
- [10] Saranphong Pramsane and Ridwan Sanjaya. "Mobile Education Services Based on SMS and Their Architecture Comparison". Third International Conference on eLearning for Knowledge-Based Society, 2006.
- [11] T. Meehinkong, P. Praneetpolgrang, K. Mekhabunchakij. "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 Society, 2009.
- [12] Tom H Brown. "Towards a model for m-learning in Africa". The International Journal for e-Learning. 2005.