JOURNAL OF APPLIED QUANTITATIVE METHODS

SECURITY EVALUATION IN COLLABORATIVE M-LEARNING SYSTEMS

Paul POCATILU[2]
PhD, Economic Informatics Department,
University of Economics, Bucharest, Romania

E-mail: ppaul@ase.ro

Cristian CIUREA[3]
PhD Candidate, Economic Informatics Department,
University of Economics, Bucharest, Romania

E-mail: cristian.ciurea@ie.ase.ro

Mihai DOINEA[4]
PhD Candidate, Economic Informatics Department,
University of Economics, Bucharest, Romania

E-mail: mihai.doinea@ie.ase.ro

Abstract: *The paper analyses the security issues related to m-learning applications. The collaborative systems are classified, emphasizing on collaborative systems from the mobile learning field. The security of informatics applications is analyzed inside an m-learning system in order to reveal vulnerabilities of different applications. M-learning applications are tested in order to discover possible security vulnerabilities. Metrics are built to measure the security level of each application and to achieve the security assessment of collaborative-learning systems.*

Keywords: *Collaborative System; Mobile Application; Software Security, Security Testing, Metric*

1. Introduction

The collaborative systems are used today in different activity fields, like banking, medicine, education, military and aviation. The educational system is a collaborative system in which new standards are needed. If the followings collectivities are considered: T - the set of teachers, L - the set of learners and S - the set of supervisors, then the collaboration exists between elements of T and L, elements of T and S and between elements of T, L and S. The design of collaborative educational systems is oriented to all partners: teachers, learners and

supervisors, and the security evaluation of informatics applications from this system is very important [1].

From informatics point of view, software applications collaborate and are integrated into an information system. Through the informatics applications that are integrated in a collaborative educational system, the share of mobile applications is reduced because the security reasons.

The mobile applications in the field of m-learning have been constructed having in mind the connection with the elements used in the learning activities, such as learners and technology users, and the control components in the learning activity system [2].

Security is a key aspect of how collaboration can be successful and fruitful for each one of the parties involved in the process of education. Security must exist as a separate layer which comes as a shell on top of the collaborative processes. Security must be considered and treated separately for each one of the aforementioned collectivities as unfolded below:

- SL – the security applied for the level associated with learners; represents measures that help individuals to benefit the most updated services and the best information in the area without any concern about the alteration and/or violation of the presented knowledge to which they must rely on;
- ST – security measures for teacher level; consists of procedures and techniques through which teachers are protected from being surprised by malicious actions of attackers; their access to mobile learning systems is regulated by means of roles and privileges, having a wide range of actions at their disposal.
- SS – security aspect for the level of supervisors; the supervisors are the ones who mediate the communication between learners and teachers by having into account the complexity of the interaction rules; the security aspects, partially should be managed by supervisors but they also must follow the rules applied to them by security measures needed to trace actions and keep logs of every operation made.

The implications of collaborative mobile learning systems from a security perspective are much greater than in a normal e-learning system due to the fact that mobile communication must also be managed by security measures additional to the ones that help and protect the communication between the application components.

2. Types of collaborative information systems

In the knowledge-based society there are encountered many types of collaborative information systems, classified by followings criteria: level of complexity, field of application and manner of organization.

Using the field of application criteria, collaborative systems are classified into several categories:

- *collaborative educational systems*, which are applied in the educational field and have the objective to evaluate and increase the performance of the educational process;
- *collaborative banking systems*, which are encountered in banking field and are used by various financial units;

- *collaborative systems of defense*, that are encountered in military field and are defined by strict rules of organizing and functioning;
- *collaborative systems in production*, their objective being to increase production capabilities and product quality within different goods and services production units;
- *collaborative functional systems*, refers to all the activities taking place in the economy, providing necessary information and overall coordination for production and finance management;
- *collaborative micropayment systems*, that allows customers and content providers to use their payment system of choice;
- *collaborative planning systems*, which present the most appropriate way to tackle certain kind of planning problems, especially those where a centralized solving is unfeasible;
- *collaborative tagging systems*, which provide a new means of organizing and sharing resources;
- *collaborative writing systems*, their major benefits include reducing task completion time, reducing errors, getting different viewpoints and skills, and obtaining an accurate text;
- *collaborative medical systems*, in which modern communication technologies allow doctors from around the world to work on the same patient, in the same time [3].

The collaborative m-learning systems are part of collaborative educational systems and refer to effective collaborative environments in which people and mobile equipment cooperate in order to achieve certain learning objectives.

These collaborative environments acts as an extension of the traditional e-learning model, providing a set of suitable tools for students and teachers to achieve their goals in anytime and anywhere manner.

M-learning or mobile learning is a new educational paradigm in which e-learning technologies are combined with mobile computing to improve the cooperation between students and teachers [4].

M-learning creates a new learning environment and allows learners to access learning material related applications anytime and anywhere through several mobile devices. Figure 1 shows the collaborative m-learning environment and its components:

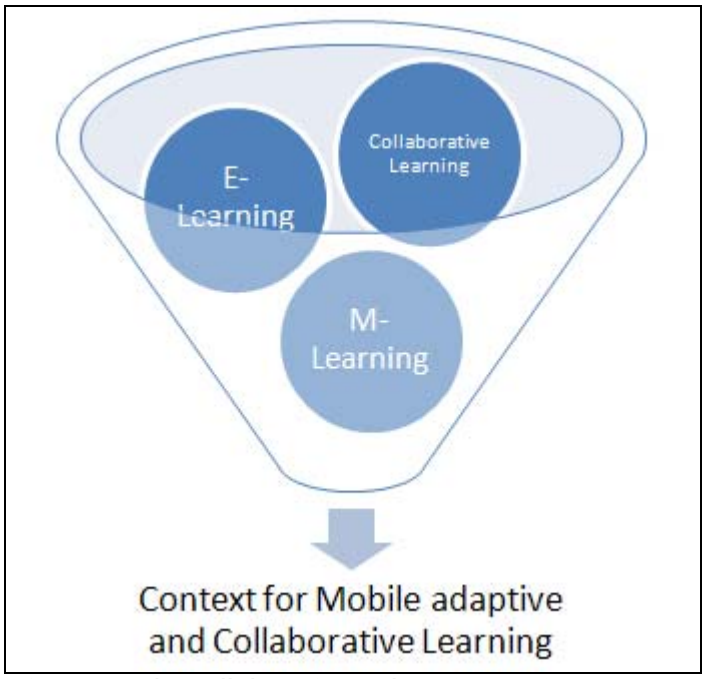

Figure 1. The collaborative m-learning environment [5]

The mobile devices, as being important components of collaborative m-learning systems, should not only provide the context information, but also must take part of the behavior adaptation, in order to achieve the given learning objectives [2].

Using mobile phones as an interactive tool for learning activities requires minimal technical and financial support because the majority of students already have the needed devices and software, and the communication occurs via existing mobile networks.

Mobile technologies contribute to promote, facilitate, and enhance student collaboration, cooperation and communication, processes that serve as a means for accessing, discovering, discussing, and sharing environmental concerns.

The role of mobile phones as a means of collaborative learning was established by the common use of these devices for facilitating friendships and socialization, in order to develop a suitable system for environmental education via mobile technologies [6].

3. Security inside m-learning systems

M-Learning systems are emerging technologies used more and more in common activities and for this reason the vulnerability level is growing rapidly as the number of mobile applications is expanding to multiple users that don't know anything about how is the backstage of such applications or what security standards could protect the user from unwanted events. Having a wide and heterogeneous users community as target, implies a special focus on technical requirements

The importance of mobile education, the process of learning by means of mobile technologies, is certified by the evolution of technology and the growing need of mobility, a direct consequence and also a demand for being efficient and obtaining the best of results.

The main advantages of mobile devices relates to hardware efficiency, portability aspects or their widespread use, features that are meant to improve the education process

quality and influence the final decision of users to implement and make use of such technologies in their everyday educative process.

The way how these mobile technologies are implemented has direct connection with the final decision with the final quality assessment of each activity which makes use of them. For this reason, security must always be carefully managed and security characteristics measured to determine the following state of attributes:

- the actual level of user's ability to trigger some unwanted actions with major impact in the final results provided by the application system's internal vulnerabilities;
- the level of threats that could virtually affect the mobile learning system's functionality;
- the degree of protection, confidentiality, of data which are sent between mobile agents.

A security event in mobile applications is described as an action which triggers a chain of undesired repercussions affecting the quality characteristics of the entire architecture. The security events for mobile applications can be classified from an affected subject perspective in:

- security events which are affecting only statically the application's functionality, with no damage on a long term view; these types of security events are usually originating inside the application and create unpleasant stops with the possibility of losing unsaved data;
- security events originated from outside the mobile application and which are, in general, driven by the malicious attacker's action; these types of security events could perpetuate and bring significant damage to users.

Security events could also originate in different types of mobile applications depending on the architecture used for developing them:

- stand-alone mobile applications; security events could be triggered by a bad implementation of the application algorithm;
- web based distributed mobile applications for mobile devices; security events are found at all levels, starting from implemented algorithm on the mobile client user up to the server on which other processes are running;
- mobile distributed architecture for Bluetooth services; security events can be triggered by a bad implementation of the communication between each device.

Collaboration in mobile distributed infrastructure needs a plus of vigilance and extra care because of the nature of the activity. The communication is vital in the collaboration process, that's way security must always be present in such applications. The access channels between mobile agents are now mature channels but still with lack of features to protect the final user. Types of different channels implement different security protocols, existing significant aspects that cannot be found all at the same technology like costs, throughput, availability, latency and others. For this developers are confronting several methods of communications like: WLAN with the standards IEEE 802.11x, WEP, WPA; Bluetooth, Infrared with IrDA or telephony GSM, GPRS, UMTS.

Types of security protocols that can be used in the implementation of collaborative M-Learning systems:

- Bluetooth security protocol for Bluetooth services [8] – implementing methods for controlling security layers for mobile learning services that are using Bluetooth protocol for communication between mobile agents;

- 3D security protocol [9] – a secure and reliable payment system, 3Domain Security Protocol, could be used for paying for educational services in a secure manner and very efficiently.

A set of security requirements that must be present in mobile applications are presented in [10] explaining why those can't be treated in general for all mobile architectures:

- authentication – feature which is required only if important information should be accessed in a restricted manner; different types of authentication can be used like: password, biometric, OTP, multi factor authentication depending on the application requirements;
- network security – is the characteristic that usually is missing or is very limited due to the technological restrictions that are still present;
- application security – for applications that are always online, the security can be controlled through a server but for the ones that aren't special rules must be applied like the concept of running into a protected environment called sandbox;
- secrecy – is given by the power in which a mobile device is able to implement encryption to protect its sensitive data;
- availability – the feature which provide permanent access to application no matter what undesired actions are taken place.

For implementing as much characteristics as possible, often multiple ways of communication between mobile agents in a collaborative process should be used in this way increasing also the complexity of the final architecture which was implemented and partially increasing also the security risks associated with possible discrepancies between used technologies.

4. Testing the security of m-learning systems

Testing the security of distributed mobile learning applications is very important and challenging compared with stand alone applications. Security testing is designed to identify security issues like:

- unauthorized access to a system or application;
- obtaining privileges in order to view and access confidential information;
- unauthorized data changes;
- prevent other users to use application (denial of services).

Figure 2 depicts a system under security test. If the attack used in a test is successfully completed (the application allows the access, although it wouldn't have) it is considered that the application is uncertain at such attacks. Otherwise, the application is considered safe, taking account of the completion of the attack [11].

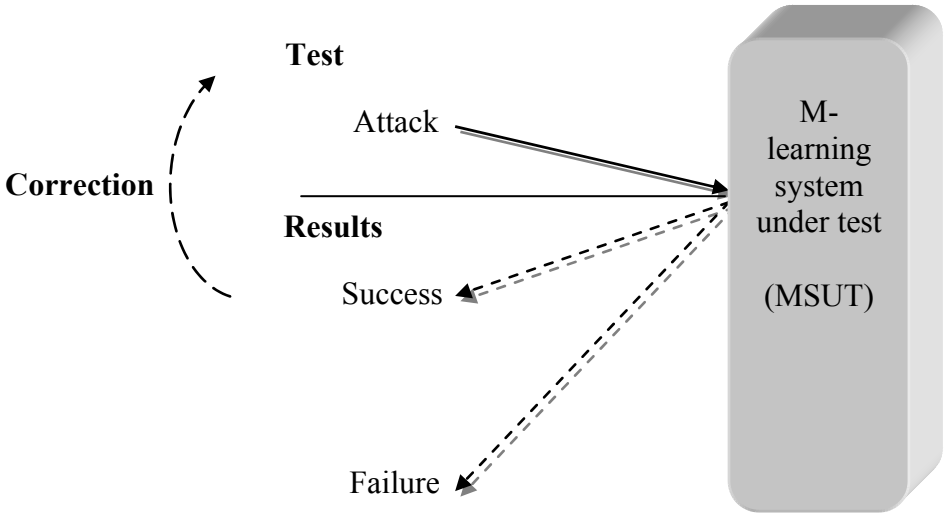

Figure 2. Security testing of IT applications

The success of an attack and is considered a failure of system security and, conversely, a failure of the attack is considered a success in terms of system security test [11]. If an attack is successfully then corrective plans and action are taken and the system is tested again.

There are several areas where the security requirements for an m-learning application are high and they need special attention.

Table 1 presents some security concerns regarding the mobile learning solutions, based on [12].

Table 1. Security concerns of m-learning applications

Action	Security requirements
Online exams	High
Homework, Projects Assessment	High
User management	High
Content management	Medium-High
Quizzes	Medium
Feedback management, Forums	Low-Medium

Each of actions from Table 1 requires a certain degree of security, depending on the importance and data sensitivity.

The databases with tests, marks and users contain sensitive data and they need a special attention. All accesses to database have to be monitored. Database security testing will focus on:

- SQL injection
- database files access rights
- unauthorized access
- data validation.

The security requirements for examinations, homework/project assessment and user management are very high due to the importance of data and information they use. Security testing involves, in addition to database security testing, identity validation and access rights checking.

The quizzes and content management have medium security requirements, because the data manipulated is less sensitive.

Feedback management and messaging for these systems usually does not use sensitive data.

These issues can be managed earlier in the development cycle using several methods and techniques like:

- different authentication levels;
- password management;
- data encryption;
- location services.

One way to simulate an intrusion attack is through penetration testing. This method leads to the identification of weaknesses of systems such as:

- vulnerable services
- ineffective security policies
- configuration issues.

Penetration testing is used for different aspects of networks and different network topologies, firewalls, operating systems and applications [11]. It is based on passwords breakers, network packet filtering and other tools.

Wireless data monitoring is very important for security testing. The majority of mobile learning applications connect to a network or Internet through wireless networks (EDGE/UMTS/Bluetooth/Wi-Fi). For an attacker it is easier to analyze wireless traffic and to access system resources. Monitoring and analyzing wireless data during the security testing can reveal security issues that need to be fixed.

5. Metrics for security evaluation

Collaborative m-learning systems have special quality characteristics, according with their field of interest.

The *security* is the main quality characteristic of collaborative m-learning systems, which require the existence of the followings: *confidentiality*, that means protecting data leaking to unauthorized parties, *integrity*, meaning to avoid data corruption and *availability*, which suppose ensuring that data and applications are always available to authorized entities with no interferences.

In order to measure the performance level of one student that give a test on a mobile device, a base question will be chosen from the test and the following indicator will be calculated:

$$PL = \frac{\sum_{i=1}^{n} p_i}{n}$$

where:

- *PL* – the performance level of the student from the collectivity that participate to the test;

- p_i – the points received by the student *i* if he give the correct answer to the base question ($p_i = 10$ if the student *i* responded correctly and $p_i = 0$ if the student *i* has given an incorrect answer).

An m-learning application for students' evaluation it is considered, based on Android operating system. For 12 students that gave a test with 5 questions, the results in Table 2 were obtained. Each question is passed (mark 10) or not (mark 0).

Table 2. The points received by students to the test questions

Students\Questions	Q1	Q2	Q3	Q4	Q5
S1	10	0	10	10	0
S2	10	10	10	0	10
S3	0	10	10	10	10
S4	10	10	0	10	10
S5	0	0	10	10	0
S6	10	10	10	10	10
S7	0	0	0	0	10
S8	10	10	10	10	0
S9	10	0	10	0	10
S10	0	10	0	0	0
S11	10	10	10	0	10
S12	10	0	10	10	0

For student S12, the performance level indicator is calculated as follows:

$$PL_{S12} = \frac{10+0+10+10+0}{5} = 6$$

The value obtained for the performance level indicator means that the student gave incorrect answer for two questions.

Another metric for assessing the security is the attack rate, *AR*, upon an m-learning application:

$$AR = \frac{NIP}{TNIP} * 100$$

where:

- TNIP – the total number of accessed IP addresses;
- NIP – the number of IP addresses from which a different type of attack was launched.

In the m-learning application for students' evaluation an encryption algorithm was implemented for increase the user security.

The attack rate metric was measured before and after the implementation of TDES encryption algorithm inside the m-learning application. Before the moment when the application was secured, the attack rate was bigger and has diminished in time. In Table 3 are presented the AR values measured between September 2009 and June 2010.

Table 3. The measured values of attack rate indicator

Month	Attack rate (AR) value
September 2009	70%
October 2009	68%
November 2009	65%
October 2009	61%
December 2009	60%
January 2010	54%
February 2010	45%
March 2010	32%
April 2010	26%
May 2010	12%
June 2010	3%

The data was automatically acquired from defects, times moments, errors, and based on their values were calculated the indicators for each metric.

For implementing security on mobile devices and maintaining in the same time the efficiency and performance of a collaborative mobile learning system, an optimization process should be carried out because of the mobile devices lack of energy. When implementing robust, but efficient encryption algorithms to protect data, the mobile processor is intensively used. That's way a security optimization process should be conducted in order to establish equilibrium between the total amounts of resources spent for implementing the security measures in collaborative mobile learning systems.

In order to measure the security efficiency for mobile devices on which collaborative learning systems are implemented an indicator should be calculated for determining if the added security is actually worth the energy spent in process it.

Let SA_i, be the security benefit for the security component S_i. If SC_i represents the security costs in terms of energy spent for sustaining and executing the security component S_i, than the security efficiency can be seen as:

$$SE_i = \frac{SA_i}{SC_i}.$$

For determining the energy costs for implementing one security feature, a simple process of measurement can be conducted by using the following algorithm as presented in [8]:

1. full charge of the device's battery;
2. measuring the amount of energy spent in processing without a security component, EB;
3. charging again the device's battery 100%;
4. measuring again the amount of energy spent in processing data but this time with the security component turned on, EA;
5. determining the amount of energy used for a specific security component AES, AES = EA – EB.

Based on the aforementioned procedure the ratio from the total amount of energy used for processing information without a security component, necessary for covering the needs for it, can be declared as:

$$S_r = \frac{EA - EB}{EB}.$$

If $S_r > 1$ than the amount of energy spent is more than twice greater than the amount used without the security component. In this case the difference of energy must be justified by the security advantage brought by the component.

When implementing a security architecture for a collaborative mobile learning system, than the total amount of resources, *TAR*, available should not be exceeded by the resources needed for running the processes together with their security features.

$$TAR > \sum_{i=1}^{n} EB_i + AES_i,$$

$$n - \text{the number of security components}.$$

The level of energy resources is highly sensitive when mobile devices are working in multithreading state, processing huge amounts of data for collaborative purposes. For this reason a collaborative mobile learning architecture should be carefully designed to relieve each one of the mobile devices caught in the process from unnecessary tasks by trying to call different services that can be run on a server.

The efficiency of security testing method (EST_i) is related to the number of security issues found in software under test:

$$EST_i = \frac{NSIi}{NTSI} \times k$$

where:

NSI_i – number of security issues found using method *i*;

NTSI – number total of total security issues found;

k – coefficient depending on the system type; it has values from 0 to 1 and it is calculated based on empirical data.

The m-learning application for students' evaluation was tested against security vulnerabilities. Two different methods were used and the results are presented in Table 4.

Table 4. The number of security vulnerabilities

	NSI	NTSI
Testing method 1	183	220
Testing method 2	197	220

The efficiency of the second testing method is calculated as follows (the coefficient *k* has been empirically established to 0.4):

$$EST_2 = \frac{197}{220} \times 0.4 = 0.358$$

The result means that the second testing method is very efficient, the value of the efficiency indicator being near to the value of *k* coefficient.

The cost of work resources involved in security testing (CST) takes into account the category of resources and the cost per unit for each category:

$$CST = \sum_{i=1}^{NC} \sum_{j=1}^{NR_i} d_{ij}\, p_{ij}$$

where:

NC – number of resource categories;

NR_i – number of resource from the category *i*;

p_{ij} – price per unit for the resource category *i*;

d_{ij} – units of usage for the resource category *i*.

In order to test the m-learning application against security vulnerabilities, the categories of resources in Table 5 were considered.

Table 5. The categories of resources used in the security testing process

Resources category	Role	NRi	Price (EUR/unit)	Units
Management	Project manager	2	20	10
	Team leader		15	20
Programming	Programmer	2	5	10
	Senior programmer		10	20
Testing	Tester 1	2	10	20
	Tester 2		14	15
Security	Specialist	1	25	10

The cost of resources involved in security testing process for the data presented in Table 5 is the following:

CST = (20 x 10 + 15 x 20) + (5 x 10 + 10 x 20) + (10 x 20 + 14 x 15) + 25 x 10 = 11410 EUR.

These metrics need to be validated using several sets of data and applying various methods and techniques.

6. Conclusions and future work

When designing a collaborative m-learning system should be taken into account the context in which it will be used and the views of the social group that will use it. Learning should be seen not only as a process of information transfer from teacher to student, but as knowledge-building process while interacting with other participants of the group to a specific educational activity [7].

The learning process from a collaborative m-learning system can be achieved through an internet mobile learning platform. The collaborative m-learning system should focus on how to instruct and stimulate learners to achieve knowledge, and the system to simulate traditional classroom education and learning environment.

The increasing adoption of mobile devices and applications, combined with the large availability of wireless technologies and networks, provide new ways for supporting learning across a variety of settings [2].

Testing the security of mobile learning systems is very important during the development. It is an expensive process and has to be planned from the earlier stages of the development cycle.

An efficient collaborative mobile learning system has to be sensitive to the context that characterizes the interactions between humans, applications and the surrounding environment [5].

References

[1] Ivan, I., Ciurea, C. and Milodin, D. **Collaborative Educational System Analysis and Assessment**, Proceedings of The Third International Conferences on Advances in Computer-Human Interactions, ACHI 2010, February 10-16, 2010, Saint Maarten, Netherlands Antilles, IEEE Computer Society, 2010.

[2] Gil, D. and Pettersson, O. **Providing Flexibility in Learning Activities Systems by Exploiting the Multiple Roles of Mobile Devices**, The 6th IEEE International Conference on Wireless, Mobile, and Ubiquitous Technologies in Education, IEEE Computer Society, 2010.

[3] Pocatilu, P. and Ciurea, C. **Collaborative Systems Testing**, Journal of Applied Quantitative Methods, Vol. 4, No. 3, 2009.

[4] Fernandes Lopes, R. and Andres Carmona Cortes, O. **An Ubiquitous Testing System for m-Learning Environments**, Second International Conference on Systems and Networks Communications (ICSNC 2007), IEEE Computer Society, 2007.

[5] Malek, J., Laroussi, M. and Derycke, A. **A Middleware for Adapting Context to Mobile and Collaborative Learning**, Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06), IEEE Computer Society, 2006.

[6] Cavus, N. and Uzunboylu, H. **A Collaborative Mobile Learning Environmental Education System for Students**, 2008 International Conference on Computational Intelligence for Modelling Control & Automation, pp. 1041-1046, IEEE Computer Society, 2008.

[7] Arişanu Lăculeanu, A. M. **Virtual communities and education**, Informatica Economica Journal, Vol. 10, No. 2 (38), 2006, Inforec Publishing House, ISSN 1453-1305.

[8] Boja, C., Batagan, L., Doinea, M. and Zamfiroi, A. **Secure Bluetooth services in an m-learning environment**, SEPADS'10: Proceedings of the 9th WSEAS international conference on Software engineering, parallel and distributed systems, Cambridge, UK, pp. 144 – 150.

[9] Yang, C. and Qi, M. **Scheme and Applications of Mobile Payment based on 3-D Security Protocol**, Proceeding Mobility '06 Proceedings of the 3rd international conference on Mobile technology, applications & systems, 2006, ISBN 1-59593-519-3.

[10] Jürjens, J., Schreck, J. and Bartmann, P. **Model-based Security Analysis for Mobile Communications**, Proceeding ICSE '08 Proceedings of the 30th international conference on Software engineering, 2008, ISBN 978-1-60558-079-1.

[11] Pocatilu, P. and Pocovnicu, A. **Mobile Learning Applications Audit Issues**, Informatica Economica Journal, vol. 14, no. 1, 2010, pp. 137-144.

[12] Alecu, F., Pocatilu, P. and Capisizu, S. **WiMAX Security Issues in E-Learning**

Systems, Proc. of 2nd International Conference on Security for IT & C in Journal of Information Technology and Communication Security, Bucharest, November 2009, pp. 45-52

[1] **Acknowledgements**
This work was supported by CNCSIS –UEFISCSU, project number PNII – IDEI 2637/2008, project title: *Project management methodologies for the development of mobile applications in the educational system*.

[2] **Paul POCATILU** graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 1998. He achieved the PhD in Economics in 2003 with thesis on Software Testing Cost Assessment Models. He has published as author and co-author over 45 articles in journals and over 40 articles on national and international conferences. He is author and co-author of 10 books, (Software Testing Costs, and Object Oriented Software Testing are two of them). He is associate professor in the Department of Economic Informatics of the Academy of Economic Studies, Bucharest. He teaches courses, seminars and laboratories on Mobile Devices Programming, Economic Informatics, Computer Programming and Project Management to graduate and postgraduate students. His current research areas are software testing, software quality, project management, and mobile application development.

[3] **Cristian CIUREA** has a background in computer science and is interested in collaborative systems related issues. He has graduated the Faculty of Economic Cybernetics, Statistics and Informatics from the Bucharest Academy of Economic Studies in 2007 and the Informatics Project Management Master in 2010. He is currently conducting doctoral research in Economic Informatics at the Academy of Economic Studies. Other fields of interest include software metrics, data structures, object oriented programming in C++ and windows applications programming in C#.

[4] **Mihai DOINEA** received a PhD scholarship from the Academy of Economic Studies, Bucharest, Romania in Economic Informatics at the UvA Research Center. He has a master diploma in Informatics Security (2006). He is assistant lecturer and he teaches data structures and advanced programming languages at the Academy of Economic Studies. He published more than 20 articles in collaboration or as single author and co-published two books in his area of interest. His research interests are given as follows: informatics security, distributed applications, optimization criteria, databases, artificial intelligence, information management, security policies, mobile devices, networking and wireless communication.