Teaching Information and Software Security Courses in Regular and Distance Learning Programs

Education Theory and Practice, Framework, and Examples

Anca-Juliana Stoica
Department of Information Technology
Uppsala University, Uppsala, Sweden
Department of Electrical and Computer Engineering
University of Florida, Gainesville, FL USA
anca.stoica@it.uu.se

Shareeful Islam
School of Architecture, Computing, and Engineering
University of East London
London, United Kingdom
shareeful@uel.ac.uk

***Abstract*—Information system security is critical to meet the growing technological needs for the industry. Information security education is necessary to support such need. However security education depends on real project context. In this article, we address the educational challenges in teaching information and software system security by presenting an education framework governed by context-driven action research used for developing modules in specific regular and distance learning programs. We differentiate issues relating to both regular and distance learning program.**

Keywords: education research framework; information and software security education; context-related action research; competency-task-context model; experiential learning; module curriculum development; module specification; regular and distance learning graduate programs

I. Introduction

Teaching information and software security is a difficult and challenging task. The main reasons are: i) the domain is very much context specific; ii) real project situation is necessary to demonstrate the security concepts within the organisation and system specific context; iii) skills to analyse security threats and risks requires time and vary from one project to another project context. Therefore, course design involving knowledge acquired in a typical classroom setting is not sufficient for such modules. It is also necessary for students to gain skills and insights typically acquired through experience. Furthermore, as distance learning is gaining popularity nowadays for both learner and institution perspective, teaching security management in distance learning program introduces addition challenges.

The need to acquire experience for identifying and analyzing security and risks is well known by educators and demanding by the industry community [7,9]. There are several reports that urge the need of information security professionals [1, 2]. Therefore information security education is timely and necessary considering state of the art. To satisfy both class room teaching and skills for security and risk management, we focus on our courses on both classroom based teaching and industry specific real life projects. This paper presents our experience as well as student learning experience related to teaching information security courses into engineering education at both regular and distance learning program levels.

II. Theory and Practice of Learning and Teaching

Learning is defined in [3] as a 'relatively permanent change in behaviour with behaviour including both observable activity and internal processes such as thinking, attitudes and emotions'. It follows that motivation is included in this definition of learning. There are different theories of learning and people use different ways to learn [5,13,15]. Here we present the theories that we use for our teaching and learning context: i) reinforcement theory; ii) facilitation theory; iii) sensory stimulation theory; iv) experiential learning. For instance we follow both positive and negative reinforcement by providing feedback to the student works. In particular positive reinforcement such as reward sometimes motivates the learners for their learning. In case of facilitation theory, instructor should act as a facilitator more able to listen to the learners and provide feedback. Therefore, reinforcement theory supports the facilitation theory. However, learners should take more responsibility for learning that is particularly importance for distance learning education. Practical experience from the case study is used for the experiential learning. In both regular and distance learning programs, several case studies are used for the course works part. Some of the case studies are selected by the students based on their working experience from the real life project while others are provided by us from different projects. Therefore, experiential learning as a part of active learning, we develop cooperation between us as an educational institution with industrial organizations. As for learners we encourage them to take responsibility for their own learning which is very much necessary for distance learning course units, and provide much of the input for the learning process which occurs through their insights and experiences.

978-1-4673-6110-1/13/$31.00 ©2013 IEEE

III. INFORMATION AND SOFTWARE SYSTEM SECURITY EDUCATION

The goal of security education is to analyze threats and risks and balance the costs associated with the implemented action to protect the risks [2]. Such education includes various domains such as software engineering, cryptography, law, management, human computer interaction, and information theory [16, 17, 18]. Based on our academic experience during the past years, we have addressed the question of how can education in information and software system security be structured and answer this question by presenting our development work in the area in a framework governed by action research. Action research is a term that was first coined by K. Lewin [12] who described it as comparative research that consists of experimenting by making changes and studying the results in a cyclic process of planning, action, and fact finding about the results of the action. These steps are illustrated within an action research cycle in our context of developing information and software security module units. Figure 1 illustrates the steps in action research connected to different theoretic perspectives.

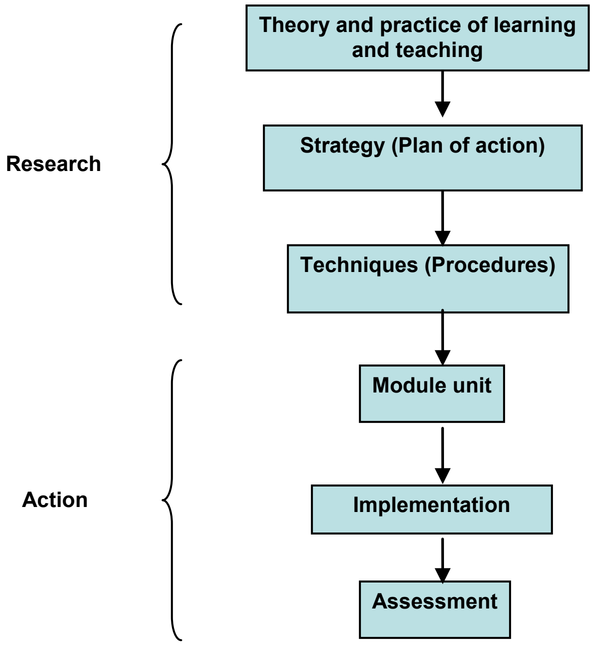

Figure 1. Context-related action research connected to theory and practice of learning and teaching information and software system security

In our curriculum development, we apply reasoning about information and software security in terms such as context and how it can be conducted [15,16]. In order to do so we first build our competency-task-context model. The model is presented in Figure 2 and relates the following concepts: *competency*, *skills, knowledge, personal characteristics / experience, tasks,* and *context*.

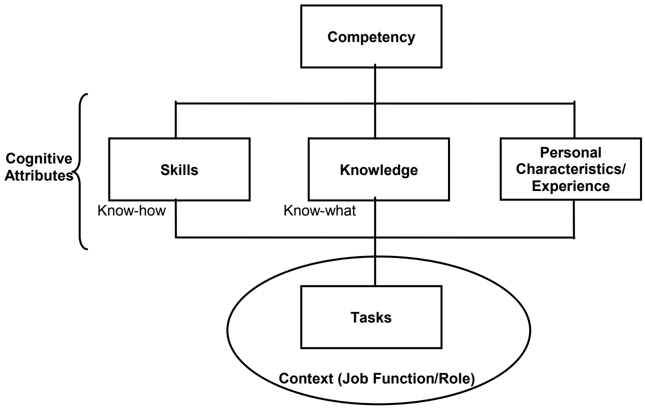

Figure 2. Competency-task-context model used for information and system security learning

Competency is the capability to choose and apply an integrated combination of *knowledge, skills*, and *personal characteristics* and traits in order to perform a *task* in a given *context*. Competency can be: *generic* (life skills) and *domain specific* (here we use domain specific competency in *information and system security*). Skills (know-how), knowledge (know-what), and personal characteristics are cognitive attributes. Personal characteristics to be mentioned here are: motivation, self-confidence, and willpower. Various approaches of competency based education are: problem-based learning; project-based education; case-based learning; dual learning with relationships in the world of work, or learning in a professional context (distance education). Competence-task-context learning model in information and system security is used for academic curriculum development by us as educational institution in cooperation with industrial organizations as depicted in Figure 3.

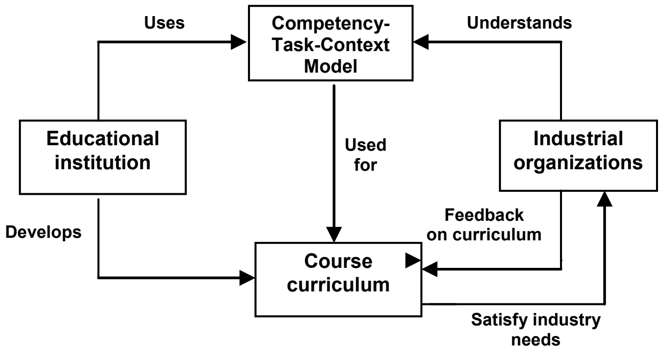

Figure 3. Course curriculum in information and system security learning and bilateral collaboration academia with industry

Figure 4 depicts the main components that we consider for the module specification. The main components are module aim, learning outcomes, assessment, and topics. These are connected to the appropriate skills (thinking skills and practical skills) necessary for the information security domain. There are two types of assessment, i.e., course work and exam. Module aims and learning outcomes are linked with the topics. Modules within the regular program consider both course work and exam. The coursework are both group and individual. For the group coursework, the pedagogical value is mainly the team structure and cooperation within the group members for the different project deliverables [4, 10]. Module specification addressing aims, learning outcomes, and course assessment are illustrated by actual examples of specific course units.

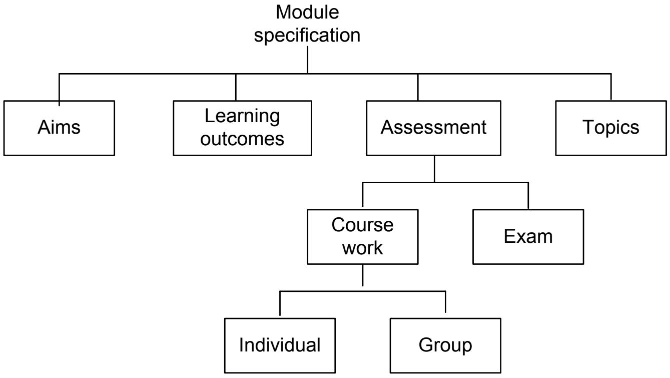

Figure 4. Components of module specification

IV Information and Software System Security Course Units

This section provides actual examples of specific course units that we cover for the learning and teaching practice.

A. *Secure Software Systems Engineering*

Secure Software Systems Engineering course unit is offered for regular M.Sc. programs such as: Information Technology and Software Engineering.

Module Aim and Learning Outcomes

The aim of this module is to provide students conceptual knowledge about analysis and design of secure software, practical experience for system design considering security, and software engineering ethics. The learning outcomes of the module focus on *knowledge* (critical concepts, principals, and practices of security and risks management, understanding ethical and legal issues of secure software development), *thinking skills* (designing secure software system using appropriate techniques and methodologies), *practical skills* (ability to analyze threats and risks for software intensive information system). The teaching and learning methods for the module are through lecturers, tutorials, practical sessions, and project works. Project works are mainly considered as a group work in real project context.

Student Groups

Working in a group is essential for software/security engineers. Each student group consists of minimum 4 and maximum 6 students. The students are required to view their groups as members of a software project. Each member is assigned different project roles. Different roles for the project are project manager, security engineering, requirements engineering, risk manager, coder and tester. Of course some members play more than one role for the successful project completion. The primary pedagogical value of the team structure is the team cooperation and communication. The communication among team members has to be undertaken in a professional way including e-mail communication, exchange of documents through cloud technology such as using dropbox, team meeting minutes and agenda focusing on project deliverables. We provide project management tool to the groups so that they can track the project progress.

Assessment

The assessment method for the module is a combination of a coursework (50%) and exam (50%). The coursework emphasizes the project work mainly assessing thinking and practical skills and the exam assesses the knowledge acquired from the module. Course work considers a project mainly focusing on web based application development. The course work consists of three different parts, i.e., part 1 and 2 belong to group work and part 3 individual evaluation. As an illustration of one of our course instances, four different projects are considered and two of them are connected to real customers: Web Based Customer Credit Control System, Online Retailer for Electronic Products, Estate Agent System Management, and Online Flash Game Students need to provide the deliverables in group work: Group code of ethics, Project goals and deliverables, Threat model, Security requirements, Risk status reports, System design, Prototype coding of agreed functionalities, Testing report, and Implementation planning. Individual deliverables include: How each member follow the group code of ethics considering his/her role; Evaluation of 2 different security and risk management methods [6, 8].

B. *Information Security Management*

This module belongs to a distance learning M.Sc. program in Business Information Technology. Students as online learners of this module are mainly working people.

Module Aim and Learning Outcomes

The module aims the need for good security management; in particular emphasize the need of network and systems management audit and to identify the problems associated with security management. The learning outcomes of the module focus on *knowledge* (i.e., critically analyze models and frameworks for information security management and employ risk management for the purpose of audit), *thinking skills* (i.e., critically evaluate security threats and vulnerabilities) and subject based *practical skills* (i.e., conduct an audit on specific system environment). The teaching and learning methods are online based in particular consists of weekly online study guides and power point slides, online hand book style content, short videos about various topics, forum discussion, Wiki areas, exercises, quizzes and glossary. We follow the virtual learning environment Moodle for managing the module content.

Assessment

The assessment method for the module is a combination of two individual course works. Both course works have several deliverables and there are is specific documentation template including sections that the learners need to follow. Coursework 1(20%) is an individual project proposal focusing on issues relevant to security management. Online learners are able to choose the proposal based on their real work experience. There are three main parts of the coursework: part 1 - motivation about selecting the topic; part 2 - critical evaluation of security threats and vulnerabilities; part 3 - challenges involving successfully implementation of the proposal with respect to security management. Coursework 2 (80%) provides students with several scenarios from real organizational specific context and learners need to choose one of the scenarios or use a scenario based on their real project works. The assumption is that the learners are working as security consultants for the scenario based system context. Three deliverables need to be produced for the coursework 2. Deliverable 1: analyze the existing ISMS practice focusing on business goals, processes, assess management, and gap analysis. Deliverable 2: perform risk management focusing on risk management scope, threats and vulnerabilities for the assets, control actions and risk status report. Deliverable 3: security policy and audit focusing on control objective, statement of applicability, control actions for the implementation of policy and risk mitigation strategy.

C. *Software Engineering and Security Architecture*

This module is part of a regular international M.Sc. program in Information and Communication Systems Security. International students are admitted based on fulfilling the program requirements.

Module Aim and Learning Outcomes

The course is an advanced course on methods, principles, modeling, design and possible pitfalls to modern software security solutions. The syllabus includes deep studies on: software security, risk management, and the role of security personnel in project teams; software system engineering and architectural principles for software security; technology selection to alleviate software vulnerabilities; system security analysis and security auditing tools; assurance criteria evaluation methods such as Common Criteria/ITSEC; stages of the software life-cycle and methods for alleviating software vulnerabilities. The learning outcomes are to enable students to identify common software vulnerabilities: their causes, symptoms, and remedies; apply secure software design methods; implementing these using appropriate architectures; relate to standards for secure software engineering; using methods to evaluate software security.

Assessment

The course is based on active learning both individually and in groups. The assessment method is a combination of individual coursework (25%), group coursework (25%), and written examination (50%). The required prerequisites are: i) successfully completion of an introductory module in IT security; ii) basic knowledge of computer architecture and the ability to read and analyze program code. Open questions and suggested research topics allow students to participate in practical project work where several methods, tools and principles are applied.

Examples of open questions are: How is security best integrated into a standard engineering-based approach; Do all engineers need to understand security; What kind of organization can build secure software; Is experience and expertise necessary for good security analysis; How does auditing designs differ from auditing source code.

Examples of suggested research topics: Quantify, analyze, and explain bug/flaw categories; Perform cost/benefit analysis proving that early is good; Untangle security software from software security at the requirements stage; Explain why the software security problems are growing and present possible remedies; Apply risk-based decision-making framework at early architectural design phase. [16, 17].

Take-home assignments are used for the individual coursework, e.g.: analyze a software product for the legitimate purpose of demonstrating that a piece of software is vulnerable and show the following: why is vulnerable; what are the consequences of the vulnerability; what countermeasures one can take to avoid the vulnerability (ies). Show the source code and text explanations about the above questions.

A final workshop is scheduled at the end of the course where students actively participate and present the results of their group work and also learn from other groups' experiences. During the workshop presentations students views regarding this module are that they have learned to solve problems and making decisions through practical application of the course material.

D. *Differences Between Traditional and Distance Education*

Computer and information security education needs to balance teaching the concepts and principles with the practice. The goals are to protect the assets from possible threats and associated risks. The presented modules focus to achieve these goals. However, there are several issues that distinguish traditional from distance education. Some of them are challenging to address distance learning programs compared to regular programs [7, 11]. Figure 5 shows the issues that use to distinguish between teaching and learning in regular and distance learning programs. Note that in Figure 5, R is used for regular learning and D is used for distance learning. Some issues are applicable for both regular and distance learning programs.

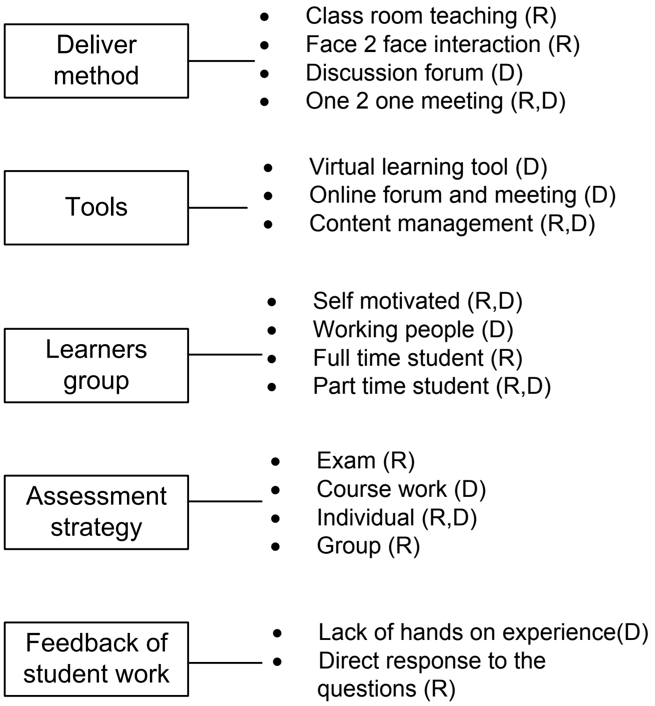

Figure 5. Comparison issues between regular and distance learning teaching modules

Deliver method
One of the main differences between regular and distance learning programs is the teaching deliver method. In case of distance learning program, there is no face to face interaction among the learners and between learners and module instructor. In addition of the face to face interaction between instructor and learner, regular program also provides interaction among the class mates.

Teaching tool
Tools certainly play one of the main roles to support the learning environment in particular for the distance learning. In our case, we use Moodle system and Skype as teaching tool for the module. Familiarity with the learning tools especially with the Moodle learning management system is necessary and prerequisite for the distance learning education. In case of teaching modules in regular program, we use university based content management system i.e. blackboard learning system, for delivering lectures, assessment information, notices and programming tools to support the practical part of the module.

Learner groups
It is necessary that learners should be self motivated for the distance learning education. Learners that have lack of motivation or lack of self direction would not be suitable for the distance learning environment. Classroom teaching and direct interaction with the instructor would be effective for such group learners. Furthermore, learners who have other commitment such as working as full time or part time, are not always able to attend regular program. These learners fit more in distance learning education. In the presented distance learning module all learners are working students.

Assessment strategy
Generally information security modules should link security concepts, assumptions, guidelines, human and organizational issues to practice and experience. Therefore, assessment strategy should focus on the problems that are related with these aspects. Our modules consider both exam and course work. However for the distance learning modules we consider that only coursework as typical classroom examination is not applicable for such context. We recommended using individual rather than group coursework as learners are from various geographical locations of the world. However, it is really hard to conclude what type of assessment strategy really fit for the distance learning program.

Feedback of student work
Feedback to the student is certainly an important component for the effective learning [14]. Learners should receive appropriate feedback for their learning. For the distance learning module one 2 one meeting is the only way to provide feedback to the student work. However in case of regular program, we also provide face 2 face feedback to the individual students about their coursework and exam. Therefore, distance learners sometimes feel that they are not getting accurate feedback similar to the regular learners. It is difficult to understand learners' behavior in such cases. This is a real challenge for distance education.

V. DISCUSSION AND LESSONS LEARNED

Teaching in distance learning program is more challenging compared to teaching in regular program. The most important part for the distance learning program is the online learners' interactions for learning. Learners' participation can be checked and monitored through classroom teaching through questions and answers and practical sessions. However it is more difficult in case of distance learning. If the interaction is poor then potential risk can be the learning outcome would not be achieved. We focus on these issues from the beginning of the semester. We follow several strategies:

Discussion Forum: Every week discussion forum is initiated with 2-3 open topics based on the week lecture content. Individual learners need to participate and respond by presenting their views on the raised open issues. The benefit of such effort is that learners need to read the lecture content before responding the open topic. It supports the student interaction and understands their view on the selected topics.

Weekly Online Discussion Session: There is a scheduled 2 hours weekly discussion session using Skype throughout the semester. Every week, we define the agenda which continues for half of the session. Students are allowed to ask questions about the lecturers, course works and clarify any other issues during the session. Most of the time final hour is a continuation of the discussion and students share their experiences about the information security incidents.

One 2 One Meeting: There is also a one 2 one discussion session for any special needs such as extra help before the coursework submission.

Networked learning is applicable for distance learning:

- activities are performed in real working environments (companies where the students work);
- electronic networks and platforms are used (e.g. Moodle);
- students can participate in learning situations in which they collaborate with students from other companies/countries that are enrolled in the same distance module;
- actual work like projects and course assignments is individual because of the students' different working environments.

Utilize learners domain expertise: As stated previously, all learners in distance learning program are working people and some of them have quite long experience working in information security projects. Therefore, they share the experience with others during the weekly discussion session. Also the problems they faced in real projects are analyzed further with us to identify the possible solution for the effective information security practice. This make the distance learning module unique compared the regular program.

VI. CONCLUSION

Computer and information security education is necessary for the growing demand of security experts from the industry perspective. Such courses should provide education on various aspects of security not only from the technical perspective but also from the management and human resource perspectives covering state of the art technology. This paper presents the steps in action research connected to different theoretic perspectives. We develop a competency-task-context model for information and software security learning and integrate it in a framework for module curriculum development as a cooperation between academia and industry. We use this framework for course module specification and apply our theory by providing actual examples of specific course units that we cover for the learning and teaching practice. Three different modules related to software and information security are presented. The modules are systematically structured. We consider modules from both regular and distance learning programs. We differentiate the issues that are relevant for both regular and distance learners**.** Learning theories like sensory stimulation, reinforcement theory, experiential learning, and facilitation theory are all applicable for the regular programs but in case of distance learning, experiential learning and reinforcement theory are very effective to meet the learning outcomes. In addition, learners should be always active and responsible for their learning outcomes. As future work we are planning to focus on quality benchmarks and student behaviour issues in the distance learning education modules related to computer and information security**.**

REFERENCES

[1] M. Bishop, "Education in information security", IEEE Concurrency, pp. 4-8, Oct.-Dec. 2000..

[2] M. Bishop, "What do we mean by computer security education?", In Proceedings 22nd National Information Systems Security Conference, Oct.1999.

[3] R. Burns, The Adult Learner at Work, Sydney, Business and Professional Publishing, 1995.

[4] B. Bogolea and K. Wijekumar, " Information security curriculum creation: a case study", Proceedings of the 1st annual conference on Information Security Curriculum Development, 2004, ACM.

[5] L. Dunn, Theories of learning. [Online] Oxford Centre for Staff and Learning Development Available at: "http://www.brookes.ac.uk/ ,2000.services/ocsld/resources/theories.html" [Accessed 5 January 2012].

[6] S. H. Houmb, S. Islam, E. Knauss, J. Jürjens and K. Schneider, "Eliciting security requirements and tracing them to design: an integration of common criteria, heuristics, and UMLsec", Requirements Engineering Journal , Vol 15, No 1, PP 63-93., 2010.

[7] S. Islam, H. Mouratidis and J. Jürjens, " A framework to support alignment of secure software engineering with legal regulations ", Journal of Software and Systems Modeling, Vol 10, No 3, page 369-394, 2011, Springer-Verlag.

[8] S. Islam and S. H. Houmb, " Integrating risk management activities into requirements engineering ", In Proc. of the 4th IEEE International Conference on Research Challenges in Information Science, Nice, France, 2010.

[9] S. Islam, H. Mouratidis and C. Kalloniatis, A.hudic, and L.Zechner, "Model based Process to Support Security and Privacy Requirements Engineering ", International Journal of Secure Software Engineering (IJSSE), Vol. 3, issue 3, September 2012, IGI Global publication.

[10] J. C. Knight and T. B. Horton, "A software engineering project course model based on studio presentations", In Proceedings of 33rd Annual Frontiers in Education conference (FIE2003), IEEE Computer Society.

[11] W. Kim and T. K. Shih, "Distance education: the status and challenges", Journal of Object Technology, Vol. 2, No. 6, November-December 2003

[12] K. Lewin, "Action research and minority problems", J.Soc.Issues 2(4), pp 34-46, 1946.

[13] McGill, I. and Beaty, L. Action Learning, second edition: a guide for professional, management and educational development, London: Kogan Page,1995.

[14] Quality isues in distance learning, AACSB International, 2007

[15] A.J. Stoica and S. Islam," Integrative educational approach oriented towards software and systems development", International Journal of Engineering Pedagogy, vol. 3, issue 1, pp. 36-43, January 2013.

[16] A.J. Stoica, Software Engineering and Security Architecture, Lecture notes, Royal Institute of Technology (KTH), Stockholm, Sweden, 2004.

[17] A.J. Stoica, "Software risk management", Lecture notes in Tools and Processes for Software, Graduate course, Stanford University, Fall 1999.

[18] W. Yurcik, D. Doss, "Different approaches in the teaching of information systems security", Proceedings of the Information Systems Education Conference, 2011.