INTED 2010

International Technology, Education and Development Conference

Valencia (Spain)
8th-10th of March, 2010

CONFERENCE PROCEEDINGS

www.inted2010.org

INTED 2010

International Technology, Education and Development Conference

Valencia (Spain)
8th-10th of March, 2010

CONFERENCE PROCEEDINGS

www.inted2010.org

Published by
International Association of Technology, Education and Development (IATED)
www.iated.org

INTED2010 Proceedings CD
Edited by
L. Gómez Chova, D. Martí Belenguer, I. Candel Torres
International Association of Technology, Education and Development
IATED, Valencia, Spain

ISBN: 978-84-613-5538-9
Depósito Legal: V-845-2010

Book cover designed by
J.L. Bernat Tomás

WELCOME INTRODUCTION

Dear INTED2010 participants,

It is a great honour to welcome you to this forth annual edition of INTED2010 (International Technology, Education and Development Conference).

The main aim of this conference is to provide an international forum, counting with experts in different fields and disciplines from more than 60 countries who will present and discuss the latest innovations in education, technology and development.

With the presence of more than 400 attendants, INTED2010 also aims to be a social platform and a great opportunity for networking, which makes this experience more interesting for its international and multicultural atmosphere.

Valencia, venue of this conference, will provide you with the opportunity to discover a city with impressive architecture, interesting museums, lovely beaches and a varied cultural offer that will make your stay unforgettable.

Thank you very much for coming to INTED2010 and for contributing to the improvement of Education with your projects and experiences. We wish you a fruitful conference!

INTED Organising Committee

SCIENTIFIC COMMITTEE AND ADVISORY BOARD

Agustín López	SPAIN
Alexander Schmoelz	AUSTRIA
Amparo Girós	SPAIN
Andrei Achimas Cadariu	ROMANIA
Anna Mazzaro	UNITED STATES
Antonio García	SPAIN
Ari-Matti Auvinen	FINLAND
Artis Ivanovs	LATVIA
Barbara Schroettner	AUSTRIA
Becky Kwan	HONG KONG
Brian McKay-Epp	UNITED STATES
Claudia Kummer	AUSTRIA
Damien Shortt	UNITED KINGDOM
David Martí	SPAIN
David Nielsen	AUSTRALIA
David Santandreu Calonge	HONG KONG
Deirdre Kelleher	IRELAND
Don Cyr	CANADA
Elena Ors	SPAIN
Fran Cornelius	UNITED STATES
Giuseppe Fiorentino	ITALY
Helen Keegan	UNITED KINGDOM
Ignacio Ballester	SPAIN
Ignacio Candel	SPAIN
Ismael Serrano	SPAIN
Javier Domenech	SPAIN
Javier Martí	SPAIN
José Antonio Arrueta	SWEDEN
Jose F. Cabeza	SPAIN
Jose Luis Bernat	SPAIN
Lasse Ziska	GREENLAND
Luciana Oliveira	PORTUGAL
Luis Gómez	SPAIN
Lyudmila Smirnova	UNITED STATES
Mª Jesús Suesta	SPAIN
Marc Seifert	GERMANY
Margarida Lucas	PORTUGAL
Maria Fojk	IRELAND
Maria Porcel	SPAIN
Mariane Gazaille	CANADA
Michael Cant	SOUTH AFRICA
Miriam Schcolnik	ISRAEL
Mohamed Elammari	LIBYAN ARAB JAMAHIRIYA
Niki Frantzeskaki	NETHERLANDS
Norma Barrachina	SPAIN
Norrizan Razali	MALAYSIA
Oge Marques	UNITED STATES
Rachid Benlamri	CANADA
Relja Dereta	SERBIA
Robert Heath	UNITED KINGDOM
Roger Bateman	NEW ZEALAND
Sergio Pérez	SPAIN
Shaibu Bala Garba	OMAN
Sharon Jumper	UNITED STATES
Silvia Ferraris	ITALY
Siobhan O' Sullivan	IRELAND
Susana Raya	SPAIN
Sven Tuzovic	UNITED STATES
Theresa Fay-Hillier	UNITED STATES
Thomas Baaken	GERMANY
Victor Fester	NEW ZEALAND
Xavier Lefranc	FRANCE

CONFERENCE SESSIONS

ORAL SESSIONS, 8th March 2010.

e-learning & Blended Learning (1)
Educational Software and Serious Games (1)
University-Industry Collaboration
Curriculum Design in Engineering Education
Architecture & Urban Planning: Pedagogical & Didactical Innovations
e-learning & Blended Learning (2)
Educational Software and Serious Games (2)
Enhancing Learning and the Undergraduate Experience (1)
Engineering Education: Pedagogical & Didactical Innovations
Architecture & Urban Planning: International Projects & Research
Pedagogical & Didactical Innovations (1)
Computer Supported Collaborative Work. Web 2.0 and Social Networking
Enhancing Learning and the Undergraduate Experience (2)
Experiences in Engineering Education
Arts & Humanities: New Experiences and Pedagogical & Didactical Innovations
Pedagogical & Didactical Innovations (2)
Computer Supported Collaborative Work
Quality Assurance in Education
Learning Experiences in Primary and Secondary School
Bus. Adm. & Mgmt.: Experiences in Education and Pedagogical & Didactical Innovations

POSTER SESSIONS, 8th March 2010.

Poster Session1. Technological Issues & Computer Supported Collaborative Work
Poster Session2. Educational Software and Serious Games & Pedagogical & Didactical Innovations

ORAL SESSIONS, 9th March 2010.

Technology-Enhanced Learning (1)
Curriculum Design and Innovation
Foreign Languages: Experiences in Education
Experiences in Education. New projects and innovations (1)
Teacher and Pre-service Teacher Education Experiences
Experiences in Education. New projects and innovations (2)
Technology-Enhanced Learning (2)
International Projects
Curriculum Design and Innovation. Strategies, Principles and Challenges
Foreign Languages: Pedagogical & Didactical Innovations
Experiences in Education
Technological Issues in Education
Barriers to Learning & Diversity Issues in Education
New Experiences for Curriculum Design
Health Sciences: Experiences and Pedagogical & Didactical Innovations
New Trends in the Higher Education Area
Research on Technology in Education
General Issues. Education and Globalization
Research in Education
General Issues. Education & Development

POSTER SESSIONS, 9th March 2010.

Poster Session1. Experiences in Education and Research & International Projects
Poster Session2. Curriculum Design, University-Industry Collaboration, Quality Assurance & Higher Education Area

VIRTUAL SESSIONS

Computer Supported Collaborative Work
Curriculum Design and Innovation
E-content Management and Development
Educational Software and Serious Games
Experiences in Education
Experiences in Education. Competence Evaluation
Experiences in Education. Enhancing learning and the undergraduate experience
Experiences in Education. Learning Experiences in Primary and Secondary School
Experiences in Education. New projects and innovations
General Issues. Barriers to Learning
General Issues. Education, Globalization and Developmnet
General Issues. Organizational, legal and financial issues
International Projects
New Trends in the Higher Education Area. ETCS experiences and Joint degrees programmes
New Trends in the Higher Education Area. New challenges for the Higher Education Area
Pedagogical & Didactical Innovations. Collaborative and Problem-based Learning
Pedagogical & Didactical Innovations. Evaluation and Assessment of Student Learning
Pedagogical & Didactical Innovations. Learning and Teaching Methodologies
Quality assurance in Education
Research in Education. Academic Research Projects
Research in Education. Experiences in Research in Education
Research in Education. Research on Technology in Education
Technological Issues in Education. E-learning and Blended Learning
Technological Issues in Education. Technology-Enhanced Learning
University-Industry Collaboration
Virtual Universities. Distance education

ABOUT INTED2010 Proceedings CD

HTML Interface: Navigating with the Web browser

This CD includes all presented papers at INTED 2010 conference. It has been formatted similarly to the conference Web site in order to keep a familiar environment and to provide access to the papers trough your default Web browser (open the file named "INTED2010.html").

An Author Index, a Session Index, and the Technical Program are included in HTML format on this disk to aid you in finding particular conference papers. Using these HTML files as a starting point, you can access other useful information relating to the conference.

The links in the Session List jump to the corresponding location in the Technical Program. The links in the Technical Program and the Author Index open the individual paper in a new window. These links are located on the titles of the papers and the Technical Program or Author Index window remains open.

Full Text Search: Searching INTED2010 index file of cataloged PDFs

If you have Adobe Acrobat Reader version 6 or later (www.adobe.com), you can perform a full-text search for terms found in INTED2010 proceedings papers.

Important: To search the PDF index, you must open Acrobat as a stand-alone application, not within your web browser, i.e. you should open directly the file "INTED2010.pdf" in the CD with your Adobe Acrobat or Acrobat Reader application.

This PDF file is attached to an Adobe PDF index that allows text search in all PDF papers by using the Acrobat search tool (not the same as the find tool). The full-text index is an alphabetized list of all the words used in the collection of conference papers. Searching an index is much faster than searching all the text in the documents.

To search the INTED Proceedings index:

1. Open the Search PDF pane through the menu "Edit > Search" or click in the PDF bookmark titled "SEARCH INTED2010 PAPERS CONTENT".
2. The "INTED_index.pdx" should be the currently selected index in the Search window (if the index is not listed, click Add, locate the index file .pdx on the CD, and then click Open).
3. Type the search text, click Search button, and then proceed with your query.

For Acrobat 9:

1. In the “Edit” menu, choose “Search”. You may receive a message from Acrobat asking if it is safe to load the Catalog Index. Click “Load”.
2. A new window will appear with search options. Enter your search terms and proceed with your search as usual.

For Acrobat 8:

1. Open the Search window, type the words you want to find, and then click Use Advanced Search Options (near the bottom of the window).
2. For Look In, choose Select Index.
3. In the Index Selection dialog box, select an index, if the one you want to search is available, or click Add and then locate and select the index to be searched, and click Open. Repeat as needed until all the indexes you want to search are selected.
4. Click OK to close the Index Selection dialog box, and then choose Currently Selected Indexes on the Look In pop-up menu.
5. Proceed with your search as usual, selecting other options you want to apply, and click Search.

For Acrobat 7 and earlier:

1. In the “Edit” menu, choose “Full Text Search”.
2. A new window will appear with search options. Enter your search terms and proceed with your search as usual.

SOFTWARE SECURITY. AN INDISPENSABLE SUBJECT FOR A SOFTWARE ENGINEER

David G. Rosado, Carlos Blanco, Luis Enrique Sánchez, Eduardo Fernández-Medina and Mario Piattini

Alarcos Research Group – Institute of Information Technologies & Systems
Dep. of Information Technologies & Systems – Escuela Superior de Informática
University of Castilla-La Mancha. Ciudad Real / Spain
{David.GRosado, Carlos.Blanco, Luise.Sanchez, Eduardo.Fdezmedina, Mario.Piattini}@uclm.es

Abstract

Computer Security has come to be of great importance given the tremendous growth of new information technologies, Web services, electronic commerce, etc. Organizations are therefore concerned about how secure their applications and infrastructures are, and what the current security level of the information systems which manage their information is. This has therefore created the need to rely on new professionals in this environment (network administrators, secure Web servers installers and supervisors, data protection, auditing, contingency, recovery, etc.).

The European Credit Transfer and Accumulation System (ECTS) is now implanted in the vast majority of the European Union's Member States and partners, and is a basic benchmark through which to achieve transparency and harmonization of their teachings. In order to implant this system of credits to software engineering, an educational innovation project has been proposed in which the guidelines to follow for the adaptation of computer engineering subjects to the ECTS system are established. These subjects will be adapted to the methodologies and techniques in accordance with the ECTS system, and a detailed planning of educational activities and continuous assessment for each subject will be implemented.

This paper presents the adaptation and implementation of a specific software engineering subject, Software Systems Security, which is part of the specific Teaching Project for Software Engineering Technology developed by identifying and adjusting the contents of this subject, first, to the guidelines defined in the ECTS system, and secondly, to the real needs that any software engineer may encounter in the present-day business world.

Keywords - Software Security, ECTS, Computer Engineering, curriculum.

1 INTRODUCTION

Software Engineers consider security to be a non-functional requirement, but unlike other non-functional requirements, such as reliability and performance, security has not been fully integrated within the development lifecycle and it is still mainly considered after the design of the system. However, security not only introduces quality characteristics but also constraints under which the system must operate. Ignoring such constraints during the development process could lead to serious problems [1], since security mechanisms would have to be fitted into a pre-existing design, therefore leading to design challenges that usually translate into software vulnerabilities [2, 3]. Moreover, a huge amount of money and valuable time are required to overcome these problems once they have been identified (a major rebuild of the system is usually necessary).

There are at least two reasons for the lack of support for security engineering [4]:

- Security requirements are generally difficult to analyze and model. A major problem in analysing non-functional requirements is that there is still a need to separate functional and non-functional requirements, while individual non-functional requirements may also relate to one or more functional requirements. If non-functional requirements are stated separately from functional requirements, it is sometimes difficult to see the correspondence between them. If stated with functional requirements, it may be difficult to separate functional and non-functional considerations.

- Developers lack expertise in secure software development. Many developers, who are not security specialists, must develop systems that require security features. Without an appropriate methodology to guide these developers during the development processes, it is likely that they will fail to produce effective solutions [5].

By considering security only at certain stages of the development process, it is more than likely that security needs will conflict with the system's functional requirements Taking both security and functional requirements into account throughout the development stages helps us limit to cases of conflict, by identifying them very early in the system development, and finding ways to overcome them.

One of the ways in which to overcome these cases of conflict is by ensuring that security plays an integral role in the education of software developers, and software engineers in particular must be conditioned to consider the security of their software products from the early stages of architecture and design.

In development environments or processes, the architecture and design phase represents a critical time for identifying and preventing security flaws before they become part of the software. As the connectivity, complexity, and extensibility of software increase, the importance of effectively addressing security concerns as an integral part of the architecture and design process will become even more critical. During this phase in the software development effort, architects, designers, and security analysts have an opportunity to ensure that requirements are appropriately interpreted through a security lens and that appropriate security knowledge is leveraged to give the software structure and form in a way that minimizes security risk [6].

With the rise of new information technologies, Web services, electronic commerce, etc., organizations do not feel secure, and trust will only be generated when it is possible to demonstrate that the overall system is secure. There is, therefore, the need for new professionals in this environment (network administrators, installers and supervisors of secure Web servers, data protection, auditing, contingency, recovery, etc.).

Given how important it is for organizations to have such professionals, and because of the increasingly important role of information technology in improving organizations' productivity, ensuring their survival, and even changing our lifestyle (eGovernment, eCommerce, etc.), the tremendous importance of the implementation of security in our modern and connected society is warranted. However, despite its great importance in the current curricula (to be removed it), it is not considered to be an important subject and is defined as a specific optional subject or as free configuration regarding security, to which very few credits are devoted, or it is referred to in a paragraph within the compulsory degree subjects, such as operating systems or networks.

By taking advantage of the establishment of new curricula, we attempt to confer upon the subject of Security the importance which it will have for future software engineers, defining it as a compulsory subject within the Software Engineering intensification of the new curriculum that we are attempting to implement in the University of Castilla-La Mancha (UCLM)'s Computer Science degree. This paper focuses on a detailed definition of the contents and activities of the subject of Software Systems Security based on the international curriculum, security standards and regulations and security specifications.

This paper is structured as follows: Section 2 defines the objective of the new European education system and the proposed new curriculum adapted to the European system for the UCLM's Computer Science degree. Section 3 presents the contents of the subject of Security Software which is a compulsory subject of 6 ECTS within the field of Specific Technology of Software Engineering. Finally, in Section 4 we present the conclusions of this work.

2 TIMES OF CHANGE

The construction of a Europe of knowledge has given rise to an important movement, which has as its goal the development of a European Higher Education Area (EHEA). This will, in turn, make it easier for qualifications to be recognised, ensuring the best possible education for students and guaranteeing their integration into a unified, borderless labour market.

The European Higher Education Area [7] sets out to establish a system of courses and credit points [8] that is common to all the EU states (ECTS – European Credit Transfer System - Credits). The EHEA solely sets out a series of guidelines and does not specify the exact content that each course should have, this task having been left to the committees of experts in each country.

What is known as the Bologna Declaration [9] sets out the objectives for the adoption of a system of qualifications that is easy to interpret, and which simultaneously makes comparisons simple. It will also set up an international system of comparable credit transfers (ECTS), to foster students', teachers' and researchers' mobility and it will encourage European cooperation in the quest to guarantee the quality of higher education. The aim, in short, is to make it possible for there to be a European dimension in higher education.

The Bologna Plan has allowed a shared European higher education policy to be formed, with the collaboration of educators, students, experts and politicians from 46 countries over a 20 year period. It is the result of an extraordinary convergence effort that is converting Article 149 of the Constitutional Treaty of the European Community into a reality, and this "will contribute to the development of a quality education system, promoting cooperation among Member States".

The principal Bologna reforms concentrate on: the three-cycle degree structure (bachelor, master's, doctorate), quality assurance in higher education, and the recognition of qualifications and periods of study. These reform efforts have created new opportunities for universities and students. The launch of the European Quality Assurance Register for Higher Education last year is helping to raise the visibility of European higher education and boost confidence in institutions and programmes, both within Europe and worldwide.

This new European education system signifies that various national and international universities are defining, updating and establishing the new curriculum in order to adapt to the European credit system (ECTS). This is the case presented in this paper: an approach for a new educational innovation project that the UCLM has developed for the degree in computer engineering in order to adapt it to the European education system and which is currently in the process of being verified by the ANECA (National Agency for Quality Assessment and Accreditation).

2.1 Proposed educational innovation project

The structure of the proposed curriculum is based on the General Secretariat of Universities' resolution of June 8 of 2009 (BOE No. 187 of 4/8/2009), which explains the degrees referred to in the aforementioned resolution. The degrees citated in this resolution are specified as:

- These are official university degree teachings, and their curriculum will consist of 240 European credits, as referred to in article 5 of Royal Decree 1393/2007 of 29 October.
- The following must be studied: the basic training block of 60 credits, the block common to the branch of computer science of 60 credits, an entire block of 48 credits for each specific technology area, and an end of degree project of 12 credits.
- The new curriculum must include at least the following modules:
    - Basic Training
    - Normal training in the branch of computer science
    - Specific Technology (at least one):
        - Software Engineering
        - Computer Engineering
        - Computing
        - Information Technologies

According to the above, the title of Computer Engineering Degree has been designed using the model of a single degree with four specializations and a list of optional courses. Each intensification contains an entire block of 48 ECTS of specific technology. The four specializations offered are: Computing, Computer Engineering, Software Engineering and Information Technology.

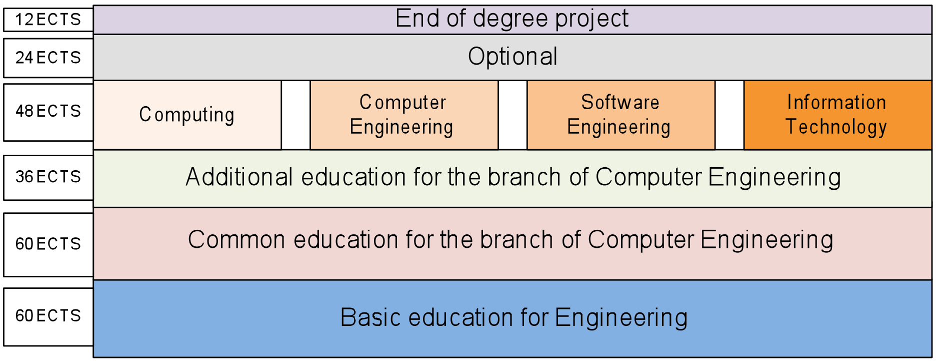
12 ECTS
End of degree project
24 ECTS
Optional
48 ECTS
Computing
Computer Engineering
Software Engineering
Information Technology
36 ECTS
Additional education for the branch of Computer Engineering
60 ECTS
Common education for the branch of Computer Engineering
60 ECTS
Basic education for Engineering

Fig. 1. Overview structure of proposed educational innovation project

As Fig. 1 shows:

- There is a basic education module of 60 compulsory ECTS.
- There is an educative module common to the branch of Computer Science of 96 compulsory ECTS, including 60 normal education ECTS in the branch of Computer Engineering which is explicit in the Council of Universities' agreement, plus a block of 36 additional education ECTS in the branch of Computer Engineering.
- There are four specific technology modules of 48 ECTS. Each includes an intensification of specific technology for each of the four offered. It is mandatory that the student takes one of these in its entirety.
- Optional subjects are offered to permit the student to cover the 24 optional ECTS included in the curriculum. Of these, 6 ECTS can be obtained as specified by the RD1393/2007 (Article 42.2.i LOU) through participation in cultural university activities, sports, student representation, solidarity and cooperation. Work experience in companies also allows students to obtain 12 optional ECTS.
- There is an end of degree project of 12 ECTS, which is compulsory for all students.

With regard to teaching methods, the training activities provided in each type of material are:

- Activities addressed.
  - Lectures. Presentation by the teacher. This will show the student the basic concepts and techniques with indications on how to complement and increase learning in the subject.
  - Seminars on issues and cases. Students will solve problems related to the material presented in lectures. In situations in which the teacher guides the resolution of problems / cases, the student must participate actively, proposing solutions, improvements, presenting possible approaches, and so on.
  - Laboratory Practices. Laboratory practices will be organized according to the contents of the materials. Students will exercise the implementation of the theoretical concepts with specific equipment.
- Supervised activities.
  - Tutorials. Individual or small group meetings in which the teacher will clarify doubts, advise on the evolution of laboratory practices and address specific issues.
- Autonomic activities.
  - Study. Individual study and development of intrinsically related tasks, including preparation of sketches, conceptual maps and summaries. Finding information, and reading books, papers and cases.
  - Troubleshooting and case preparation. This is individual or group work, which on the one hand, complements studying in itself and, on the other hand, is part of the previous work on problems and case seminars.

- Preparation of laboratory practices. Preparation of laboratory practices individually or in small groups. This consists of reading the script of the practice, the answers to the questions raised therein and the realization of a work plan for the efficient use of the laboratory meeting. A practical memory is then written.

- Evaluation activities.
    - Assessment. Written and/or oral test.

Also related to teaching methods are the possible systems of assessment depending on the materials. These are:

- Written and/or oral tests. Mid-term and final exams.
- Submission of reports, problems, etc. Submission of short reports on specific topics.
- Laboratory work and/or cases. An evaluation of the previous preparation of the practice, the ability to carry it out efficiently and the quality of the analysis reflected in the report will be assessed.
- Presentations and participation in seminars. Previous preparation of the exercises/cases assigned to the session and contribution to the collective discussion will be assessed.

After presenting the new curriculum to be evaluated and implemented during 2010/2011, the focus of our study is to provide a detailed description of the contents of one of the subjects that we believe to be important and which is part of the intensification of Software Engineering. This is Software Systems Security, to which we now turn.

3 SOFTWARE SECURITY

The aim of this paper is to provide a detailed presentation of the contents and activities in the subject of Software Systems Security, which is framed within module III concerning specific technology (see Table 1), and in which we can see that security software has been included in the specific technology of Software Engineering as a compulsory subject of 6 ECTS in the proposed new curriculum.

Module III (Specific Technology) has 48 ECTS, and four implementations of this are performed (to cover the four specializations offered), which can be seen in Table 1. The European diploma supplement will note the intensification carried out by the student in the implementation of each specific technology module.

Table 1. Content of the Module III

Module	Area	Subject	ECTS
Module III-SE. Specific Technology of Software Engineering (48 ECTS)	Specific Technology of Software Engineering	Requirements Engineering	6
		Software Design	6
		Database Development	6
		Enterprise Information Systems	6
		Software Engineering Processes	6
		Software Systems Security	6
		Software Systems Quality	6
		Software Systems Security	6
Module III-CE. Specific Technology of Computers Engineering (48 ECTS)	Specific Technology of Computers Engineering	Operating Systems II	6
		Microprocessor-based System Design	6
		Network Infrastructure Design	6
		Network Management	6
		Advanced Computers	6
		Network Security	6
		Embedded Systems	6
		Systems and Services Planning and Integration	6
Module III-CO. Specific Technology of Computing (48 ECTS)	Specific Technology of Computing	Automata Theory and Computation	6
		Compilers	6
		Algorithm Design	6
		Multi-Agent Systems	6
		Knowledge-Based Systems	6
		Interactive Systems Design	6
		Data Mining	6
		Declarative Programming	6

Module III-IT. Specific Technology of Information Technologies (48 ECTS)	Specific Technology of Information Technologies	Integration of Computing Systems	6
		Network Design and Management	6
		Information Systems Management	6
		Web Technologies and Systems	6
		Multimedia	6
		Computing Systems Security	6
		Human-Computer Interaction II	6
		Electronic Commerce	6

The subject of security attempts to include all the most important aspects of security that are required by society for future software engineers. The proposed content is based on different standards, international curriculum and security specifications that we consider to be most important, and are most often used by both national and international companies and institutions in which the figure of the software engineer is necessary.

A high-level description is defined in the new curriculum (descriptors) for this subject, in which the content consists of: i) Fundamentals of security, ii) Organizational Security iii) Security requirements iv) Security in software development; v) Security of information systems; vi) Security risks vii) Security services; viii) Security management and ix) Certification, regulations and standards for the security.

The aim of this subject is to enable students to identify, model and integrate the software security requirements into the development process, learn the main techniques and software security services, and discover the rules, standards and most significant legislation on software security.

We shall now provide details of each of these descriptors, indicating the most appropriate contents and those that fit what is dictated by the rules and security standards [10-15], and the most important international curriculum [16-22].

A. Fundamentals of Security

The CS2008 curriculum [21] defines the discipline of “Programming Fundamentals”, in the area of “FoundationsInformationSecurity” which defines topics as such: Role and purpose of computer and network security; Security goals: confidentiality, integrity, availability triad; Security standards and policies; Security mindset; Defence in depth; Common threats: worms, viruses, trojans, denial of service; Security versus usability, time, and/or money tradeoffs. Furthermore, in the “Information Assurance and Security” discipline of IT2008 [22], there are areas related to security such as Attacks, Fundamental Aspects and Security Mechanisms (Countermeasures).

The most appropriate contents according to the knowledge areas of the different international curriculum for this descriptor are, therefore, the following:

- Concepts of Computing Security
- Principles of computing security: Confidentiality, Integrity and Availability.
- Risk factors: Environmental, technological and human.
- Security mechanisms: preventives, detectives and correctives.
- Security threats

B. Organizational Security

ISO/IEC 17799:2000 considers the organization as a whole and takes into account all possible aspects which may be affected by any incidents that may occur. Under this standard, the topics related to the organization are: Security policy; organizational aspects with regard to security; asset classification and control, and security related personnel. This standard attempts to provide a basis through which to take into consideration every aspect that may involve an incident in an organization’s business activities.

The most appropriate contents according to this standard for this descriptor are, therefore, the following:

- Introduction to organizational security
- Security policies and procedures

- Classification and control of assets
- Personal security

C. Security Requirements

The Common Criteria (CC) [14] is an international standard (ISO/IEC 15408) for computer security. Its purpose is to allow users to specify their security requirements, to allow developers to specify the security attributes of their products, and to allow evaluators to determine whether products actually meet their claims. It also presents requirements for the IT security of a product or system under the various categories of functional requirements and assurance requirements. Moreover, in the Software Engineering discipline of the CS2008 curriculum [21] one of the topics in the ”RequirementsSpecifications” area is: Functional and non-functional requirements.

So, by following the recommendation of these standards and international curriculum, the most appropriate contents according to this descriptor are the following:

- Concept of non-functional requirements
- Requirements Engineering
- Definition and classification of Security Requirements
- Security Requirements Engineering techniques and models
    - Misuse Cases
    - Common Criteria
    - SQUARE

D. Security in software development

The SE2004 curriculum [19] is focused on Software Engineering and defines security aspects such as Systems development (e.g. security, safety, performance, effects of scaling, feature interaction, etc.) in the “Engineering foundations for software” unit; Analyzing quality (non-functional) requirements (e.g. safety, security, usability, performance, root cause analysis, etc.) in the “Analysis fundamentals” unit; Design for quality attributes (e.g. reliability, usability, maintainability, performance, testability, security, fault tolerance, etc.) in the “Software Design” unit; and Testing across quality attributes (e.g. usability, security, compatibility, accessibility, etc.) in the “Testing” unit. In the “Software Engineering” discipline of the CS2008 curriculum [21] there is also an area dedicated exclusively to the definition of software processes which is “Software Processes”, and whose topics are: Software life-cycle and process models; Software process capability maturity models; Approaches to process improvement; Process assessment models; Software process measurements. Moreover, an area related to the security, which is “RobustAndSecurityEnhancedProgramming”, defines topics such as: Defensive programming; Principles of secure design and coding: Principle of least privilege and Principle of fail-safe defaults; How to detect potential security problems in programs; How to document security considerations in using a program. Finally, the “Analysis, Modelling and Design” course of the MSIS2006 curriculum [16] defines topics such as: Systems development Methodologies; Requirements determination; Team organization and communication; Feasibility and risk analysis; Design reviews; Systems development life cycle; Conceptual and logical data modelling.

Therefore, when considering the aforementioned aspects in relation to software engineering, it is necessary to focus in greater depth on the aspect of security and its incorporation into software developments. The contents for this descriptor are, therefore:

- Introduction to software development
- Secure software development
- Security approaches in development processes

E. Security of Information Systems

The “Algorithms and Complexity” discipline of the CS2008 curriculum [21] defines security areas such as “Cryptographic Algorithms” with topics such as: Historical overview of cryptography; Private-key cryptography and the key-exchange problem; Public-key cryptography; Digital signatures; Security protocols. Different security areas are also defined in the “Operating Systems” discipline, such as “Security models” with the following topics: Models of protection; Memory protection; Encryption;

Recovery Management; Types of access control: mandatory, discretionary, originator-controlled, role-based; Access control matrix model; Harrison-Russo-Ullman model and undecidability of security; Confidentiality models such as Bell-LaPadula; Integrity models such as Biba and Clark-Wilson; Conflict of interest models such as the Chinese Wall. The “Net centric Computing” discipline defines the “Network Security” area with topics such as: Fundamentals of cryptography: Secret-key and Public-key algorithms; Authentication protocols; Digital signatures; Network attack types: Denial of service, flooding, sniffing and traffic redirection, message integrity attacks, identity hijacking, exploit attacks (buffer overruns, Trojans, backdoors), inside attacks, infrastructure (DNS hijacking, route blackholing, misbehaving routers that drop traffic), etc.); Use of passwords and access control mechanisms; Basic network defence tools and strategies: Intrusion Detection, Firewalls, Detection of malware, Kerberos, IPSec, Virtual Private Networks, and Network Address Translation; Network Resource Management policies; and Auditing and logging. Moreover, in the “Social and Professional issues” discipline, we can find the “Security Operations” area which contains the following topics: Physical security; Physical access controls; Personnel access controls; Operational security; Security policies for systems/networks; Recovery and response; Dealing with problems (both technical and human). In the “Systems and Application Specialties” discipline of the SE2004 curriculum [19] we can find a speciality of “Highly secure Systems” with one of the topics of Cryptography, cryptanalysis, steganography, etc., and in “Financial and e-commerce systems” speciality topics such as Depth in security are defined. Finally, the IT2008 curriculum [22] defines the “Information Assurance and Security” area in which one of the topics is cryptography, and Security and protection is one of the topics in the “Operating Systems” area for the “Platform Technologies” discipline.

The topics recommended by the International curriculums therefore lead us to conclude that the content of this descriptor is the following:

- Introduction to Security in Information systems
- Physical and Logical security
- Cryptography
  - Symmetric and Asymmetric cryptography
  - Public Key Infrastructure (PKI).
  - Digital certificate.
  - Certification Authorities
  - Digital signature
- Security in Internet
  - Secure e-mail
  - WWW
  - Virtual Private Networks
- Security in Operating Systems
- Security in Databases

F. Security Risks

In its “Software Engineering” discipline, the CS2008 curriculum [21] defines an area of “risk assessment” in which the topics are: Definition of terms: in security, vulnerability, threat, security breach; in safety, hazard. The concept of risk; hazard and risk identification; Risk analysis including evaluation; Need for a system-wide approach including hazards associated with tools; Risk and immature technologies; Cost/benefit analysis; Principles of risk management. The learning objectives for these topics are: To define the concepts of hazard and risk, hazard; To recognize common security risks in at least two operating systems; To describe the categories of threats to networked computing systems; To display a systematic approach to the task of identifying hazards and risks in a particular situation; To apply the basic principles of risk management in a variety of simple scenarios including a security situation. A “Software Project Management” area is also defined, in which one the topics is Risk analysis, with subtopics such as: The issue of security; High integrity systems, safety critical systems; and the role of risk in the life cycle. Finally, the MSIS2006 curriculum [16] and the SE2004 curriculum [19] define “Risk management” as being the contents of “IS Management” courses and the

“Project planning” unit respectively. The ISACA Model Curriculum for Information Security Management [23] also defines the topics of risk management and risk assessment in the domain of Information Risk Management.

Based on the aforementioned contents, the structure of this descriptor is, therefore, as follows:

- Introduction to security risks
- Risk analysis
- Risk management
    - MAGERIT
    - ISO/IEC 27005:2008
- Risk assessment and cost-benefit analysis.

G. Security Services

In the “Information Assurance and Security” discipline of the IT2008 curriculum [22] there is an area called “Security Services” in which topics such as Availability, Integrity, Confidentiality, Authentication (source reliability),Non-repudiation are defined. Moreover, the “Integrative Programming and Technologies” discipline also defines an area of “Software Security Practices” with topics related to security such as: Authentication to system resources and services; and Encryption of data between systems and services. Finally, in the ITU_T X.800 [24] and X.805 [25] standards a set of security services (both Basic and advanced) are defined.

For this descriptor the most appropriate contents, following the recommendations of these curriculums and standards is, therefore:

- Security as Services
- Security Basic Services
- Security Advanced Services

H. Security Management

In the discipline of “System Administration and Maintenance” of IT2008 [22] the Security management topic is defined in the Administrative Activities area. In the ISACA Model Curriculum for Information Security Management [23] the topics of Information security management overview; Measuring information security program management; Implementing information security management are defined in the Information Security Program Management domain. The subtopics defined for these topics are: Importance and outcomes of effective security management; Organizational and individual roles and responsibilities; Information security management framework; Measuring information security management performance; Common information security management challenges; Determining the state of information security management; Information security management resources; Information security management; Implementing information security management (e.g., action plans, policies, service providers, assessments). Finally, the ISO/IEC 13335-1:2004 [11] and ISO/IEC 27001:2005 [12] standards provide an in-depth description of the management systems.

If we consider the topics and subtopics defined in the international curriculums which are related to security management, the contents can be established as follows:

- Management and Planning of the IT security
- Techniques for the management of the IT security

I. Certifications, regulations and standards for the security

The ISO/IEC 27000-series comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This series provides best practice recommendations for information security management, risks and controls within the context of an overall Information Security Management System (ISMS), which is similar in design to the management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series). There are different assessment criteria such as: a) Common Criteria for Information Technology Security Evaluation (CC) [14]. b) ISO/IEC 15408, Evaluation Criteria for IT Security. c) Information Technology Security Evaluation Criteria (ITSEC). There are also numerous assessment methodologies such as: a) Common Methodology for

Information Technology Security Evaluation (CEM). b) ISO/IEC 18045, Methodology for IT Security Evaluation [26]. c) Information Technology Security Evaluation Manual (ITSEM). Finally, many other standards and specifications related to security are defined such as the X.800 ITU_T family [25], ISO/IEC 13335 [11], and so on.

The most appropriate contents for this descriptor, which offer in depth knowledge of the most important security certifications and standards are, therefore, the following:

- Certifications of Security
- Specifications and standards of Security

4 CONCLUSIONS

The adaptation of the new curriculum makes it the perfect time to incorporate and adapt a number of subjects to the Computer Science degree. These are subjects whose importance has, over recent years evolved and increased, and have consequently not been sufficiently considered in existing curricula, and should be studied by future software engineers in order to ensure their success in the professional world. This is the case of the subject of security, which attempts to provide the student and future professional with knowledge and techniques, and guides the most important and most frequently sought security aspects of software systems demanded by most companies and organizations in today's society.

We therefore believe that it is essential for Security to be included in Computer Engineering as a compulsory subject, with a large weight in credits that will allow extensive training in both theory and practical cases, as a result of the needs which are being observed in the professional market. Universities are increasingly recognising this great demand and are expanding their range of security-related subjects in order to implant them in the new curriculum.

This is the case of the UCLM, where the new curriculum for the Computer Science degree, adapted to the European system, has been defined, and attempts have been made to establish a compulsory subject of 6 ECTS related to the security of software systems in which the most important and relevant aspects to security are provided and through which it is hoped that future software engineers will obtain a broad knowledge of this area.

5 ACKNOWLEDGMENT

This research is part of the following projects: QUASIMODO (PAC08-0157-0668) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" (Spain), MEDUSAS (IDI-20090557) financed by the "Centro para el Desarrollo Tecnológico Industrial. Ministerio de Ciencia e Innovación (CDTI)" (Spain), SISTEMAS (PII2I09-0150-3135) financed by the "Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha" (Spain), y BUSINESS (PET2008_0136) financed by the "Ministerio de Ciencia e Innovación" (Spain).

References

[1]. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Jonh Wiley & Sons, Inc, 2001.

[2]. C. Artelsmair and R. Wagner, "Towards a Security Engineering Process," Proc. The 7th World Multiconference on Systemics, Cybernetics and Informatics, 2003, pp. 22-27.

[3]. H. Mouratidis and P. Giorgini, Integrating Security and Software Engineering: Advances and Future Vision, Idea Group Publishing, 2006.

[4]. B.W. Lampson, "Computer Security in the Real World," IEEE Computer, vol. Vol. 37 (6), 2004, pp. 37-46.

[5]. J. McDermott and C. Fox, "Using Abuse Case Models for Security Requirements Analysis," Proc. 15th Annual Computer Security Applications Conference, IEEE Computer Society, 1999, pp. 55-66.

[6]. J.H. Allen, et al., Software Security Engineering: A Guide for Project Managers, Addison Wesley Professional, 2008.

[7]. EEES, “Espacio Europeo de Educación Superior,” http://www.eees.es/.

[8]. ECTS, “European Credit Transfer System,” http://www.ects.es/.

[9]. “BOLOGNA FOLLOW-UP GROUP: Work Programme 2004-2005,” 2005; http://www.bologna-bergen2005.no.

[10]. COBIT 4.1, “Control Objectives for Information and related Technology,” 2007; www.isaca.org.

[11]. ISO/IEC, ISO/IEC 13335-1:2004, Information technology - Security techniques - Management of information and communications technology security, 2004.

[12]. ISO/IEC, ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements, 2005.

[13]. ISO/IEC, ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management, 2008.

[14]. ISO/IEC, Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), 2009.

[15]. ITU, ITU_T Recommendation X.800. Security Architecture for Open Systems Interconnection for CCITT Applications, 1991.

[16]. ACM/AIS, MSIS 2006: MODEL CURRICULUM AND GUIDELINES FOR GRADUATE DEGREE PROGRAMS IN INFORMATION SYSTEMS, 2006.

[17]. ACM/AIS/AITP, IS 2002. Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems, 2002.

[18]. ACM/IEEE, Computer Engineering 2004. Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering, 2004.

[19]. ACM/IEEE, Software Engineering 2004. Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering, 2004.

[20]. ACM/IEEE, Computing Curricula 2005. The Overview Report, 2005.

[21]. ACM/IEEE, Computer Science Curriculum 2008, 2008.

[22]. ACM/IEEE, Information Technology 2008. Curriculum Guidelines for Undergraduate Degree Programs in Information Technology, 2008.

[23]. ISACA, ISACA Model Curriculum for Information Security Management, 2008.

[24]. ITU_T, Security Architecture for Open Systems Interconnection for CCITT Applications, 1991.

[25]. ITU_T, “ITU-T Recommendation X.805. Security architecture for systems providing end-to-end communications,” 2003.

[26]. ISO/IEC, ISO/IEC 18045:2005. Information technology -- Security techniques -- Methodology for IT security evaluation.