Development of Capstone Projects on Secure Communications for Engineering Students

V. Gayoso Martínez¹, A. Hernández Encinas², L. Hernández Encinas¹, A. Queiruga Dios², I. Visus Ruiz²

¹Dpt. Information Processing and Coding, Applied Physics Institute (CSIC), C/Serrano, 144, Madrid, Spain. E-mail: {victor.gayoso, luis}@iec.csic.es Tel. +34 915618806 (Ext. 418), Fax: +34 914117651

²Dpt. of Applied Mathematics, E.T.S.I. of Béjar, University of Salamanca C/Fernando Ballesteros, Béjar, Spain. E-mail: {ascen, queirugadios, ivisus}@usal.es Tel. +34 923294500 (Ext. 2223), Fax: +34 923408127

Abstract—A capstone project is a compulsory requirement for passing the last course and obtaining the bachelor’s degree. In order to make students develop their own self-learning capabilities, it is important to offer them real life projects, helping them in the process of combining already acquired information with new knowledge. In this contribution, we present the details of a real capstone project about secure communications in order to illustrate the capstone project process.

Keywords—Capstone project, collaborative education, secure communications, teaching resources.

I. INTRODUCTION

The Bologna Accord proposes an agreement on a common model of higher education with the creation of a common European area of university studies. It emphasizes the creation of a European Area of Higher Education (EAHE) as a key to promote students’ mobility, aiming to simplify Europe’s educational qualifications and ensuring that credentials granted by an institution in one country are comparable with those earned elsewhere [2].

Spain is one of the 46 countries involved in the Bologna Process. The cornerstones of such an open space are mutual recognition of degrees and other higher education qualifications, transparency (readable and comparable degrees organised in a three-cycle structure) and European cooperation in quality assurance.

The Information and Communication Technologies (ICT) and their use are considered a requisite for the adaptation to the EAHE. Technology development facilitates new strategies of communication for University studies that must be adapted to the international European context. Modern e-Learning technology may act as a bridge: On the one hand, computer systems make real experiments available over the Internet, any time, anywhere, and –even more important– make the measured data electronically available for further analysis. On the other hand, a model for an experiment can be implemented as a simulation within a virtual laboratory, making the same physical quantities available for measurement as in the real experiment [5].

One of the fields of greater projection and impact in the future, within the ICT, is Cryptography and Information Security. Its aim is the preservation of information, including the characteristics of confidentiality, integrity, and authentication. The goal of Cryptography is to provide safe communications on insecure channels, allowing people to send messages by means of a channel where the communication can be intercepted by a third person (mail or e-mail, telephone, fax, etc.), so only the authorized receiver can recover the messages [11]. The great importance of Information Security nowadays is derived from the proliferation of personal computers and the easy access to the Internet. This easiness has also brought serious problems of security, like virus, spam, phishing, publication of confidential information, etc. All of it makes necessary that students and future professionals are conscious of the dangers that Internet browsing without safety measures poses.

The capstone project provides the students the opportunity to improve different skills, which probably have not been completely developed in the habitual frame of the traditional education. The example project presented in this contribution consists of the analysis of the shortcomings and gaps related to the ICT security in Small and Medium-sized Enterprises (SMEs), in Spain, describing how to make them more secure. Since most engineers prepared at the School of Industrial Engineering in Béjar start their working life in SMEs, this particular capstone project generates really useful knowledge that can be applied to the student’s future professional work.

The rest of the paper is organized as follows: In Section 2, we will comment on the changes that are happening in the Spanish Universities in order to adhere to the European Area of Higher Education. The proposal, development, and completion of the example capstone project are presented in Section 3, while the assessment process is detailed in Section 4. Finally, the conclusions will be shown in Section 5.
II. CHANGES IN HIGHER EDUCATION

A. New teaching-learning process

In the Spanish universities, changes are taking place driven by the new technologies. We are developing new ways of relationship with our students, offering them web-based classes together with the traditional classes assuming that Information and Communication Technologies (ICT) and computers are a significant part of our daily life. The goal is to guide the students in his learning process and to give them the tools so that they can construct their own knowledge.

The growth and degree of development of ICT are modifying the classical teaching way and the form in which the students get the contents of the subjects. ICT are becoming more and more important in the higher education process, claiming new spaces and conditions of learning, and new professional roles for lecturers [3]. Their wide diffusion and direct application increase their social impact as well as their educational importance.

Nowadays, traditional education is changing to become an ICT based education. The new role of the teacher is to be a mediator in the student's knowledge construction: Rather than a dispenser of knowledge, the teacher is a guide, facilitator, and co-explorer who encourages learners to question, challenge, and formulate their own ideas, opinions, and conclusions, adjusted to the processes of learning by means of the use of the ICT. Finally, it is important to take into account that the ICT do not require of the invention of new methodologies, but it allows a modification in the strategies for the continuous learning of the student [7].

Knowledge is acquired through involvement with content instead of imitation or repetition. Learning activities are characterized by collaboration with others, this is a learning theory called Constructivism. Students should be able to apply what they learn in the University to the different situations that they might encounter over the course of their working lives. The traditional textbook guided classroom has unfortunately failed to generate the desired outcome of producing independent thinking students.

B. Tools to create a new working environment and help students to acquire knowledge

One of the new methodologies useful for engineering students is online education, which refers to the learning methods that, at least, partly utilize the ICT available through the Internet. What we propose to the students is to use the online methods together with their acquired knowledge to get a more complete education in specific issues.

Technology represents proactiveness and progress, values that are still very much ubiquitously held, where progress is simply taken to be improvement over current local conditions. As the developers of new products and processes, engineers are a driving force for innovation in today's society. In doing their work, they rely on a large amount of information from external sources, of which the web is among the most important ones [6].

As the students, tutors are using the Internet for professional networking, learning from one another about the new media and their applications to education [15]. This skill allows the students to apply the know-how to the daily work and renew their knowledge in virtually any field of investigation.

In engineering disciplines, web-based educational tools could help to ameliorate the deficit in the traditional education. Specialized knowledge can be transferred all over the world via the Internet, and new software and tools in general can be part of a comprehensive engineering higher education. In order to be able to use different software and hardware, the students need a moderate level of media competence. In addition, work-flows provided to the students must be flexible enough and be conveniently updated. Virtual teaching environments are useful and represent an important part of the engineers’ education. With the help of the new media, the transfer of knowledge could be much more illustrative and instructive than printed media.

However, the examination results of traditional mode students and online mode students are very similar and only some minor differences are reported in reference to results [13]. This suggests that there are no significant differences in overall performance between them.

III. PROPOSAL AND DEVELOPMENT OF A CAPSTONE PROJECT

Engineers typically work in order to find solutions to practical problems by applying their mathematical and scientific knowledge. The Accreditation Board for Engineering and Technology has defined engineering as "the profession in which knowledge of the mathematical and natural sciences, gained by study, experience, and practice, is applied with judgment to develop ways to use, economically, the materials and forces of nature for the benefit of mankind". Similar statements can be found on most engineering college websites, in introductory engineering textbooks, and in the mission statements of many engineering professional societies [10].

In general, secure online communication with customers, colleagues or other workers is essential in the current collaborative way of working [4], [10]. Security in the management and storage of data is also very important. We discuss in this section the particular case of a capstone project focused on the security aspects of an engineer working in a Small and Medium-sized Enterprise (SME).

A. Justification of the project

The industrial, mechanical, telecommunication and other engineers are accustomed to using confidential non-public documents or private information in varying degrees. For this reason, they must apply the needed level of security in all of their transactions and activities. University cards, credit cards, or the Spanish electronic identity card (DNIe) are some examples of security tokens that we can use, not only locally, but also through Internet without having to be presented physically.

In this capstone project, we have analysed from a global point of view the security requirements that must be taken into account by an SME, particularly when the communications are made through Internet. In this sense, it is necessary to consider the measures aimed at minimizing
the most important threats to the security. We can list the following generic types:

- **Service interruption.** This threat means that a part of the system is not available during some time.
- **Data interception.** In this case, a non-authorized person accesses to part of the information.
- **Document modification.** This thread is produced when a non-authorized entity not only accesses to the information, but in addition is able to modify its content.
- **Identity impersonation.** In this situation, a non-authorized entity sends messages impersonating a legitimate user.

B. Objectives and methodology

The purposes and objectives proposed for the example capstone project could be summarized as follows:

1. Perform an initial study of the security weaknesses of the SMEs.
2. Study the possibilities offered by the existing cryptographic techniques in order to make the enterprise more secure.
3. Provide a list of tools to ensure security in the enterprise.

The methodology to be used in order to fulfill the objectives mentioned above is characterized by the following steps:

1. Analyse the requirements for achieving secure communications and storage of information in a Small and Medium Enterprises. In particular the digital information that they possess and share with others. This could be done with a survey to some of the nearby businesses.
2. Study the existing cryptographic techniques, detailing the most important and useful in this context.
3. Consider the main cryptographic protocols related to the information security, specially digital signatures.
4. Analyse the possible usage of the Spanish national identity card (DNIe) as a security token used to sign documents.
5. Obtain conclusions to be presented to the SMEs in order to increase the security level of their information systems and communication protocols.

The following subsections describe how to achieve the proposed objectives along with the methodology used.

C. Project development

The first step in carrying out this capstone project has been conducting a survey to SMEs, taking into account that, in Spain, a company is considered to be a SME if it has fewer than 250 employees. Some of the suggested questions for SMEs that we have considered were:

- Do you know the meaning of terms like security, data encryption, digital signature, malware, phishing or spam?
- What kind of security measures do you have in the company?
- What security measures do you think would be necessary in your company?
- When managing customer data, are you aware if the data is encrypted?
- Do you use a password for logging into your PC? How often do you change it? Do your colleagues have a different key?
- Is there a password for the accounting program of the company? How often do you change it? Who knows that password?
- Do you use any security tool? Have you heard of PGP, electronic signatures or USB encryption tools? Do you have a smart card reader to use the DNIe in the Internet transactions?
- Do you have an antivirus installed in your PC? Do you know if your antivirus software allows you to filter or block certain websites?
- Is there any employee in charge of the system security? Have you received any training specifically focused in security?

Once the existing deficiencies and gaps related to the contacted companies are known, the next step consists of preparing a report detailing these deficiencies and the possible solutions.

As conclusions of the survey, we found that most employees have certainly heard of security measures, digital signatures, phishing or spam, but however they do not know how to deal with them.

Most of the workers have an antivirus in their PCs, but they usually do not know all the possibilities offered by the software such as blocking certain web pages or filtering the access to others.

The next step in the capstone project consists in studying the elements that compose a secure working environment. From that study, the final step is to provide a list of tools that can fulfil the security requirements detected in the SMEs. In the next paragraphs, the list of security elements and available tools is presented.

1) Communication security

In order to get a secure communication with another party (a customer, employee, etc.), it is necessary to fulfil the following requirements [14]:

- **Confidentiality:** Nobody apart from the legitimate users must be able to access to the information. The confidentiality of data can be achieved by using cryptographic systems.
- **Integrity:** Sureness that information has not been altered since the data was created. Integrity requires that information can be modified only by authorized entities.
- **Authentication:** This property requires both the identification of the sender (e.g. biometric procedures, passwords, etc.) and of the message (through digital signatures, etc.).

2) Cryptography

In this context, it is important to consider which is the mechanism that could provide both security and trust on the Internet environment, taking into account that the Internet is known as “the network of networks”; a set of interconnected
networks, which is open, independent, heterogeneous and universal. It is an environment that is driven by demand, not supply.

Cryptography represents the only method by which businesses can work in a secure way comparable to traditional paper based mechanisms, and its objective is to assure the secrecy and confidentiality of communications between several users [9]. Cryptographic methods are typically developed in response to the needs and demands of businesses.

It is necessary for the workers of a company to get up-to-date with security topics, especially with the two types of cryptography that are used nowadays. The first type is called symmetric or secret key cryptography, and it uses one common key for both encryption and decryption. The second type is the public key cryptography (also known as asymmetric cryptography), and it uses two different keys (a private key and a public key) in order to transform plaintexts into ciphertexts [8].

3) Data security

Concerning the security that involves the engineer’s work in a SME, we have analysed and installed in our laptops several tools, for example PGP (Pretty Good Privacy), which is a software that provides security in communications, together with cryptographic privacy and decryption. The software PGP allows the encryption of data, files and messages.

Another example of security software that can be found in the Internet is Remora USB Disk Protection. This software can protect and encrypt all the data stored in the computer, or files that are in the USB disk.

4) Digital signatures

One of the problems that arise in public key cryptography is that anyone with access to a public key directory also has access to the public keys of other users, so a person can send a message instead of another. Fortunately, as public key schemes allow to sign a message, any user is able to check not only who is the sender of a message but also the integrity of that message [12]. Thus, the electronic signature can be used to identify the author of a document, to show compliance (or disagreement) with the content, and to indicate that it has been read [8], [9].

The importance of digital signatures lies in the fact that it can have the same validity and significance of a handwritten signature. Any digital document or message can be digitally signed without the people involved having to meet in person. The digital signature can be performed, for example, with PGP or GnuGPG software, so it is not necessary to install any additional software.

5) DNIe

The DNI is a card issued by the Spanish Government that authenticates its holder as genuine and justifies the citizens’ identity [1]. Since its development (more than 50 years ago), the DNI has been an essential document to officially justify, not only inside Spain but now also in the European Union, the holder’s identity. Furthermore, the DNI guarantees the personal details showed on the card and the Spanish citizenship of its holder.

The Spanish Government has prepared a public key infrastructure that provides the new identity cards (DNIe) with the necessary technology. By using a computer with Internet connection, a card reader, and the DNIe, any worker can perform more than 800 procedures with the Government Administration with equal validity that the one provided by handwritten signatures and physical accreditation.

D. Conclusions from the project

SMEs are made up of workers with basic knowledge of computers. We have studied the needs and secure training required by those workers of a small company. Some of the security breaches that have been identified for the case of engineers and SMEs, are due to employers not updating their security measures. In fact, the only security they consider most of the time is the use of antivirus software, but they do not use any program for sending/receiving secure email or encrypting sensitive customer information when they have to transport it, either on a USB drive, a CD or any other external memory device.

Some of the employees of the surveyed enterprises are beginning to use the DNIe for business through the Internet, but there are few who currently do that.

The proposed security recommendations are cited in this project. Since technological progress is advancing rapidly in Spain, we believe that these measures are an easy way to establish a security environment, not requiring much work from the end user. The only time consuming-requirement is the training in security, but the knowledge derived from that training can be quickly integrated into the worker’s daily routine.

There are several companies that are specialized in offering technological solutions in the field of the security, focused in the SMEs, continually evaluating commercial systems in a changing sector in which innovation plays a key role.
After the presentation and the round of questions and answers is finished, the board members must decide the qualification given to the student in a closed session. The general criteria of evaluation depend on the Centre where the lecture takes place.

In case of not obtaining the approval of the examining board, the student must prepare and submit a new project about the same topic.

In the particular case of the projects described in this study, the examining board focused in three aspects: Documentation, project presentation, and the actual work performed. Concerning these elements, both the report organization and writing style were considered correct, the content was found adequate (given the student’s background) and related to his future work, the presentation was determined to be clear and well organized, the technical capabilities of the student were correctly tested during the questions and answer session, and the conclusions were aligned to the proposed objectives.

V. CONCLUSIONS

The student developing the capstone project should question the gathered knowledge and look at it from a different perspective. As future engineers, it is expected that students work deeper to understand the situations and problems that they will find in his daily work. In order to do so, it is necessary to develop certain skills in the research field.

This paper outlines the skills and knowledge that an engineer must reach in the security field. This study has analysed the security that must be taken into account in the activities in which an engineer is involved, and how they can improve the communication security.

The proposed capstone project and its development allow an engineer to be aware of his security needs, learning the tools, concepts and improvements that enable a secure working environment with no major threats.

ACKNOWLEDGMENT

This work has been partially supported by Ministerio de Ciencia e Innovación (Spain) under the grant TEC2009-13964-C04-02, by Ministerio de Industria, Turismo y Comercio (Spain), in collaboration with CDTI and Telefónica I+D under the project Segur@, CENIT-2007 2004, and by the Project FS/5-2009 from “Fundación Memoria D. Samuel Solórzano Barruso”.

REFERENCES