DIGITAL SECURITY TRAINING LABORATORY

Ander Garcia, Carlos Lamsfus
Visual Interaction and Communications Centre - VICOMTech
San Sebastián, Guipúzcoa, Spain
{agarcia, clamsfus}@vicomtech.es

Abstract

The number of computers located at schools, universities and training centres has increased greatly during the last years due to the investment accomplished by institutions. We have focused our research on Vocational Training Centres, where teachers are in charge of the installation, configuration and maintenance of IT resources. These teachers have only received basic training and are lacking of specific computer formation. Needless to say, the situation leads to bad configurations and dangerous security holes on the network of the centres.

In a previous project we established a learning platform at a Vocational Training Centre to foster a culture of digital security. We developed two digital security courses, a basic one and another one directed to network administrators. The main characteristics of the platform and the courses were a) virtual tutors, b) an advanced interactive interface, c) animations and simulations. After evaluating this infrastructure among the teachers of the vocational training centre, we detected some limitations of the simulations used on the exercises for the network administrators. We realized a more real system was required to improve the training.

In this paper we describe the digital security training laboratory developed to improve the formation of network administrators of vocational training centres. We proposed an architecture with a distributed laboratory and a centralized tutor. The tutor must be an expert on the area and his first task consists on defining the exercises network administrator have to complete to be able to properly configure the equipment of their centres (certification authorities, firewalls, ...).

The tutor's next task is to install all the necessary software in a server and create an image of it. Besides, the tutor has to create and distribute virtual machines to the students, so they are able to complete the practices using their local machines. Using the image a server is installed at each centre. All the students of each centre complete the exercises against this server. To evaluate the users, they must send to the tutor some proofs of their results (screenshots, configuration files...).

Fulfilling the tasks described on the exercises of the training, networks administrators will become capable of understanding and properly configure and maintain their systems using basic and advanced techniques.

Keywords
eLearning, digital security, laboratory

1. INTRODUCTION

We have focused our research on Vocational Training Centres, where although the number of computers has increased rapidly during the last years, teachers lacking of specific computer formation are in charge of the installation, configuration and maintenance of IT resources. In a previous project [1] we established a learning platform at a Vocational Training Centre and developed two digital security courses to foster a culture of digital security. Analyzing the results of an evaluation of the project, we realized more real and practical exercises were required to improve the training of the students.

Although we though about blended learning [2] as the solution for the problem, we then discarded it because the difficulties found to gather all the students both at the same time and at the same place. Mixture used of blended learning and videoconference was discarded too because the time restriction.

Finally we decided to develop a digital security training laboratory to improve the formation of network administrators of vocational training centres. We proposed an architecture with a centralized tutor who controls the distributed laboratory located at each centre and distributed servers and virtual machines.

This paper is organized as follows: first, we described the results of the related previous project. Next we present the digital security training laboratory, explaining the steps and actors involved on its development. At section 4 and 5 we summarize our work and the acknowledgement and references section concludes the paper.

2. PREVIOUS WORK

The main characteristics of the platform [5] and the courses developed in a previous project are a) virtual tutors, b) an advanced interactive interface, c) animations and simulations.

Students using this platform will be both assisted and guided by virtual tutors. The main objective of using the virtual tutors in this eLearning platform is the enhancement of the effectiveness of the learning experience by adding details and completing the information the user sees in the images, animations and general slides.

The interface reproduces the real environment without performance penalization, increasing the platform's user friendly features as well as the users' satisfaction. Besides it is dynamic, i.e. there are some changes depending on the hour of the day and the season of the year.

Animations and simulations mainly appear when a concept, a device or a process is being explained. Moreover they are used as interactive exercises to test the knowledge acquired by the learners during the course. They give the student the opportunity to fulfil a real task in a semi-real environment such as to create a rule to filter some e-mail address or to add a user to the system and change his/her password.

The architecture of the LMS is based on Microsoft technology, with a IIS server and a Microsoft SQL Server. The platform uses a .NET web service on the LMS and an intelligent Java applet on the Client to be SCORM [3] conformance and it has been SCORM 1.2 certified.

3. LABORATORY

The distributed digital security laboratory has been developed to improve the training of network administrators. Due to the complexity of the related tasks, it was no possible to correctly simulate the instalattion and configuration of the tools required to manage the equipments of a computer network. Network administrators require real practices to learn, practices where they can solve real situations (filtering P2P programs, securing a network, …) they are going to face at their networks and with real feedback if they make mistakes (computer hangs, connections problems, …).

There are several steps involved on the development of this laboratory. In the first step, the tutor or digital security expert has to define the exercises and the topics that the course will cover. This work is based on the course created on the previous project and its main points are:

- Secure installation, configuration and management of the OS;
- Secure communications: certificates, SSL, VPN;
- Firewalls and proxies.

Another task involved in this step is to decide the evaluation method that will be used to score the students. We are going to use screenshots and configuration files to prove the job has been well accomplished. For example, in the VPN practice, a screenshot showing that somebody has acquired the same rights that somebody would have as a user of a local machine of the remote network will be required.

The next step is to install all the necessary software to run the practices. As the course involves both Windows and Linux OS, two different servers must be installed and configured with the required applications (SQUID, Apache, SQLServer , …). An image of each server will be created to distribute among the different training centres. At each centre they will use the images to replicate the servers within their own networks. A disk image is a computer file containing the complete contents and structure of a disk and it allows to create exact copies of the original disk.

The servers must have the same hardware to avoid configuration incompatibilities when installing the image. The characteristics of the servers are the followings: Pentium IV 3 GHz CPU, 1 GB RAM and 60 GB hard disc.

Besides the server at their centre, the students will have some virtual machines installed at their computers. A virtual machine can be seen as a computer completely defined and implemented in software rather than hardware. Using these virtual machines, they can locally configure the Windows or Linux applications suited for each one of the practices. If they make a virtual machine to crash, they can reinstall it and start the practice again without affecting the stability of the network.

Students will have permissions to change the images installed at their computers but they will no be allowed to manage the server. The server will be used as a connection point to check whether the practice is correctly finished. For example, a SSH server will run on it and the students will have to connect to it and capture a screenshot to prove they have fulfilled the SSH client practice.

The tutor has to check thoroughly that the source server of the image has been properly configured and that all the practices can be accomplished without problems. Otherwise if a bug or misconfiguration is detected, a new image has to be created and distributed again to each one of the centres. The same applies to the virtual machines, but this case is even worst because the new virtual machine should be reinstalled at every computer of every centre.

Once the servers are installed and configured, the students will work with their virtual machines and against the server of their centre.

The tutor will help them to fulfil the practices and to solve any problem they may cause on the virtual machines or the server due to incorrect actions, i.e. wrong changes to OS configuration files. At each centre there will be a person in charge of the server. In case a severe problem is detected he will be responsible for reinstalling the server using the image given by the tutor.

The local virtual machines and the installation of the "wrapped up" server at each centre assure the quality and speed of the communication and protect the students against external events such as ISP or remote networks problems. Although there will be multiple students, as they will only manage their own computer and they will have no administrator permissions on the server, no control over the access synchronization to the server is required.

Should practices in the future require any administrative work on the server by the students, the different vocational training centres will have to coordinate them using various mechanisms: i.e. booking, assigning fixed times to each student…

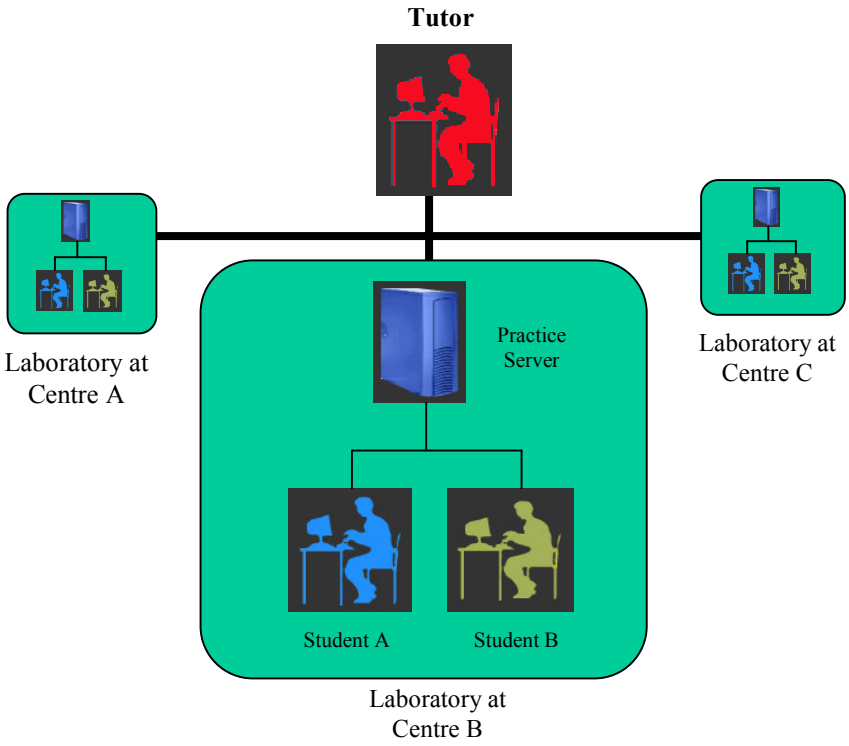

Fig. 1 Laboratory

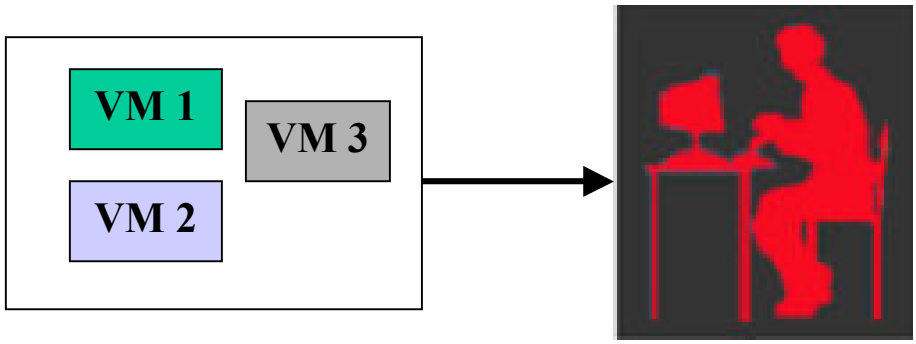

Fig. 2 Student's PC

The previous figures show the architecture of the laboratory and each of their computers. As a summary note the centralized tutor [Fig.1] who covers all the centres. At each centre there is the same server installed and all the students of the same centre connect to the server of their centre. Students have a number of virtual machines [Fig.2] installed at their computers. These virtual machines are used to fulfil the task described at the course's programme.

In this architecture the communication between the tutor and the students is even more important than in courses of other subjects. Thus, we are improving the communication tools of the platform. Asynchronous tools (forums, emails …) do not give all the required functionality [3]. Imagine a student is installing a program and he has a problem. If he has to send a mail or a forum message at each step and wait till a response is received, the installation is going to take too long. A chat can solve this, but if there are various students each one with different problems it could be chaotic.

Due to this, we are developing an instant messaging tool that allows a synchronous one-to-one communication, personalizing the learning experience of the students and giving the tutor an efficient tool to communicate and motivate each of the students.

4. RESULTS

The laboratory is at the last stage of development and it will be evaluated by around 15 users who are actually engaged with the network administrator course. A final evaluation report will be done by October. The results of the evaluation will be the input to improve both the practices and the laboratory itself before the final version of the laboratory.

5. SUMMARY

In a previous project we detected more efficient and realistic practices were needed to improve the eLearning training of network administrators. A distributed digital security training laboratory has been developed to solve this issue. There is a centralized tutor who controls the whole architecture and decides whichs practices have to be done and what infraestructure is required. He creates an image of a server with the necessary software and this server is replicated at each center. Virtual machines are created too and they are installed at students' computers. Students work against the server of their center using their virtual machines to complete the course, fullfiling real tasks and having the opportunity of consulting a digital security expert to solve their doubts.

6. ACKNOWLEDGEMENTS

The digital security laboratory has been developed inside the ELEARSEC II project. This project has been financed by the Local Government of Gipuzkoa, the Basque Government's Education, Universities and Research Department and FEDER. VICOMTech has worked with IFPS Tolosaldea, a vocational centre where the system is being evaluated, and S21Sec, a company focused on digital security.

References

[1] Garcia,Ander, Lamsfus,Carlos., “An eLearning Platform To support vocational training centers on digital security training with virtual tutors and graphical spatial metaphores “, *ISBN: 84-933971-6-4* ,IADAT-e2005, Biarritz, July 2005, pp 117-121

[2] Christian Bunse, Ines Grützner, Michael Ochs, Christian Peper,Silke Steinbach-Nordmann, “Applying a Blended Learning Strategy for Software Engineering Education”, CSEET’05 1093-0175/05

[3] *Scott Frees, G. Drew Kessler, "Developing Collaborative Tools to Promote Communication and Active Learning in Academia", 34th ASEE/IEEE Frontiers in Education Conference, Savannah, GA, October 20 – 23, 2004,*

[4] SCORM*:* ***http://www.adlnet.org***

[5] *Tolosaldea:* ***http://www.tolosaldea-birtuala.com***