A Milestone-Driven Approach for Lab Assignments Evaluation in Information Security

David Nuñez, Francisco Moyano, Ana Nieto, Juan J. Ortega, Isaac Agudo, Javier Lopez

Abstract: *In this paper we describe a methodology for designing and evaluating lab assignments based on the fulfilment of milestones. The approach relies on the integration of ICTs with an automatic, milestone-based evaluation. The final goal of this methodology is to diminish educators' workload on lab assignments, so they can focus on the development of the assigned tasks, and to enhance students' experience by providing direct and real-time feedback on their progress. This approach encourages autonomous learning on the students and optimizes the time invested by the educators during the lab assignments. In order to validate our proposal we have applied this methodology in several courses related to Information Security. The results of this experience show that the methodology improves students' performance, while facilitating the work of the educator.*

Keywords: *Milestones, Evaluation methodology, Information Security.*

INTRODUCTION

The methodology described in this paper is oriented towards enhancing the preparation and monitoring of practice assignments, particularly in the field of Information Security courses. From the feedback received in previous courses, we realized that a key factor for the proper operation of these courses consists of optimizing the design of the lab assignments and of offering real-world projects, closer to the business context where students will have the demonstrate the skills acquired throughout their formation.

During the development of lab assignments by students, we find that is necessary an almost permanent supervision of their progress, which is a costly task when the number of students is high. However, due to the fact that most of lab assignments have a sequential nature, it is possible to identify a sequence of technical milestones that all students must go through. In other words, lab assignments are usually divisible in phases that need to be correctly implemented in order to guarantee the attainment of the next phases. For this reason, it is necessary to offer feedback to the students on the state of their work, preferably in real time and in an automated manner. This feedback is extremely useful to facilitate their progress and to minimize the probabilities of stagnation.

The innovative approach that we propose in this work enables the educator to focus on the design of the lab assignments, the identification of the milestones and the associated evaluation criteria, saving time from the supervision of the progress of students, which is a high time consuming task. This approach can be easily mapped to different Information Security courses, where it is of paramount importance both the use of labs and to optimize the time spent on preparing, coordinating and doing the lab assignments.

Additionally we present three sample activities of application of the methodology corresponding to the following Information Assurance and Security Knowledge Areas (IAS KA) of the ACM Computer Science Curricula [1]: Cryptography, Network Security and Web Security. Finally we discuss the results of the pilot experience in three different courses in the last academic year.

METHODOLOGY

We propose a milestone-based methodology that integrates automated evaluation technologies in order to supervise the tasks accomplished by the students. In our methodology, students are presented with several milestones that must be performed in order to finish the assignment, allowing the professor to control the students' progress through the achieved milestones. Moreover, we also focus on providing students with feedback in case they find difficulties in achieving a milestone. The aim of this feedback is encouraging students to adopt an independent learning attitude. The educator becomes a coach in charge of supervising the evolution of the students over their milestones.

The advantage of this approach is two-fold: on the one hand, it facilitates the monitoring of the progress and the level of fulfillment as well as it encourages the independent learning; on the other hand, it makes easier for the educator to evaluate the performance of the students: not only can the educator evaluate the achievement of the practice, but also the spent effort. Likewise, this methodology may provide the educator with useful statistical information, such as how many times students tried reaching a milestone, the results of the last try or the employed time, among other information.

In order to make evaluation easier and as automatic as possible, we suggest the integration of technological support as a core part of the methodology. In this direction, we intend to design, deploy and maintain a controlled environment for the accomplishment of lab assignments by means of virtualization technologies.

Our methodology can be divided into the following steps:

1. Problem analysis and milestone decomposition.
2. Dependencies identification.
3. Milestones mapping to learning objectives/competences.
4. Identification of practical objectives for each milestone.
5. Technical binding of the milestone.
6. Definition of feedback strategy.
7. Evaluation criteria.

The first step consists of analyzing the problem and decomposing it into milestones. At this point, if the problem does not fit a milestone decomposition strategy, it maybe better to follow another approach. Usually, milestones follow a sequential order, meaning that students must build new milestones upon already-achieved ones. However, other kind of dependencies may be found, including milestones with no dependencies with others that would allow the students to choose among a set of milestones. The goal of the second step is finding these dependencies. Milestones must serve a purpose from a didactic point of view; therefore, the third step is aligning the learning objectives with the milestones, defining also the theoretical background needed by the students in order to fulfill the milestones. The fourth step is defining the technical requirements that will check off the milestones as accomplished, and it includes identifying technological support to implement these requirements. The following step comprises the technical binding or implementation of the milestone in the context of the chosen technology. This same technology may determine the feedback strategy that can be implemented in the next step. Feedback

strategies include how to communicate the progress status to students and the reinforcement strategy that will support the autonomous learning. A second objective of the feedback strategy is providing educators with the progress of their students, both at a global and individual level. Finally, it is required to define an evaluation criteria according to the evaluation of the milestones. Concretely, it is interesting how to forward individual evaluations of milestones up in the decomposition chain until reaching a global evaluation of the problem.

Note that the decomposition in milestones is a recursive progress, that is, the approach can be applied to resulting parts of the decomposition. A criterion for finishing the decomposition could be reaching a level where the implementation of the milestone on the chosen technology is straightforward.

RELEVANT LAB ASSIGNMENTS FOR IAS KA

The methodology is analysed based on our personal experience in information security and assurance courses. Three practical experiences were chosen based on their suitability to the IAS KA. Moreover, all the courses implement the methodology following a backbone of general assumptions, where the milestones generated may be reused in the different areas with a different impact.

At the beginning of the course, the student receives a virtual machine with the software installed, a guide to solve the problems requested and a questionnaire that must be completed and submitted as part of a report at the end of each practice. In the guide the main objectives and the correspondence with the competences of the course are described. Moreover, with the aim of evaluating the effectivity of the different milestones in the learning process, different approaches were considered, always related with the theoretical content and competences.

While the first assignments designed are related with the main tools that will be used during the course, including cryptographic techniques and traffic analyzers, the final milestones are focused on awakening the critical spirit of the student, to be prepared for analysing threats and countermeasures in a real system. In this way, the results of the simpler assignments (scheduled at the beginning of the course) can be used to solve more advanced assignment by the end of the course.

We used to Moodle platform [3] to implement our assignments, not only because it the virtual education platform used in our institution but also because huge community behind it and a high number of plugins available. We mainly made use of the following Moodle activities: Assignments and Quizzes.

The following three selected assignments represent relevant examples on how to design milestone-driven activities.

Assignment 1: Implementing Encryption Algorithms - Cryptography

In this use case, the lab assignment consisted in the implementation of a set of encryption algorithms. These algorithms are of deterministic nature, so for a specific input, they will have allways the same output. Thus, we can consider a more general use case that

subsumes this one, where the assignment consist on implementing a set of deterministic algorithms. For designing this assignment, first, the set of algorithms that the student had to implement was identified. These algorithms can have different completion phases. For each of them, a set of random inputs was prepared and its output was collected and matched to the correspondent input. Using this set of inputs and outputs we prepared customized questionnaires in the Moodle platform that were used as an automatic evaluation mechanism. This way, each time a student wants to evaluate his assignment, he answers the questionnaire using the output from his implementation of the algorithm, which must match the pre-computed output. The student receives immediate feedback about his implementation, and depending on the degree of granularity used for designing the assignments, he can get an idea of the state of completion of the assignment.
In a later phase students were also asked to generate a pair of public and private keys by themselves, submitting the public key together with a form for certification using the Moodle platform. In all following assignment students were requested to submit all documents digitally signed with their private key and encrypted with a public key provided by the professor.

Assignment 2: Configuring Networks - Network Security

In this case, the assignment consisted in achieving a correct network configuration of a machine for the IPsec protocol [2]. Thus, the objective is to learn how to configure a network host correctly using IPsec. In the first phase, the students have to configure its machine for connecting with other students; the goal of this phase is to familiarize students with the environment and the basic concepts behind the assignment. Next, a more advanced exercise was proposed, where students had to configure correctly their machine in order to be able to connect to a specific server. Once the connection is successfully achieved, the server asks for a validation code provided by the Moodle platform and that is unique for each student. The server checks the validation code and produces an unique response code, which is submitted to the Moodle platform in order to automatically grade the completion of the assignment. Thus, the assignment is considered complete and correct when the connection and the validation is achieved.

Assignment 3: Learning to secure web applications - Web Security

WebGoat [4] is a deliberately insecure web application maintained by OWASP and designed to teach web application security lessons. The information is organized in milestones that are checked off once students accomplish them. The first milestone involves reading some description about a vulnerability, being this description usually accompanied by screenshots. Once students understand the vulnerability from a pure theoretical perspective, they can move on to the next milestone, which comprises the actual experience with such vulnerability. In order to achieve this, the platform include already-deployed web applications that suffer the vulnerability and which can be exploited by the students. Therefore, students can experience real-life examples of insecure applications and the consequences of the vulnerabilities of such applications. Once students have exploited the vulnerability, this milestone is checked off and they can move to the next phase, where they have to fix the vulnerability. At this point, the platform provides hints to students on the parts of the code that should be modified. The last milestone is accomplished when the students try to exploit the vulnerability on the now fixed web application, and when they check that it is not vulnerable anymore.

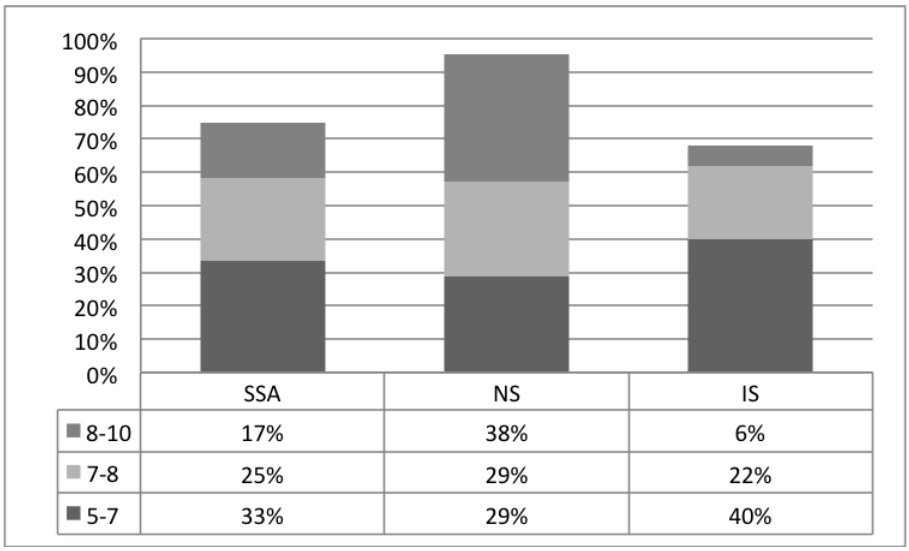
The experience of WebGoat represents well the philosophy behind our approach, as it provides a controlled, milestone-based environment on its own. It comprises a systematic approach that encourages independent learning. Students are aware of their progress at every moment and they can request some help from inside the platform if they get stucked. The educator can also see the evolution of the students by checking the list of accomplished milestones and by reviewing the corresponding part of the source code.

RESULTS AND CONCLUSIONS

Our pilot experience has covered three different courses in three different degrees, covering most of the areas of the IAS KA. The total number of students was 121, distributed as following,

- 47 in Security of Services and Applications (degree of Software Engineering).
- 51 in Information Security (degree of Informatics).
- 23 in Network Security (the degree of Telematics).

When we finished the pilot we were able to analyse the result of the proposed approach based on the success ratio (Figure 1). We have also identified some problems and challenges with the first pilot and define mechanisms to overcome them. In base of our experience we have planned some modifications to the lab assignments and the contents of the subjects involved.



	SSA	NS	IS
8-10	17%	38%	6%
7-8	25%	29%	22%
5-7	33%	29%	40%

Figure1. Percentual Results per Course

Taking into account the good results of our pilot experience we think that the same approach could also be applied to other subjects, in particular those related to programming skills. This publication can help encouraging other teachers to apply this approach at least in a partial way, providing some guidance in the process.

The results of this experience show that the methodology improves students' performance, while facilitating the work of the educator.

ACKNOWLEDGEMENTS

This research has been conducted under the Universidad de Málaga Teaching Innovation Project PIE13-166. This work is partially funded by Universidad de Málaga, Campus de Excelencia Internacional Andalucía Tech, and by FETCH European Thematic Network.

REFERENCES

[1] ACM/IEEE-CS Joint Task Force on Computing Curricula. 2013. Computer Science Curricula 2013. ACM Press and IEEE Computer Society Press. DOI: http://dx.doi.org/10.1145/2534860

[2] Doraswamy, Naganand, and Dan Harkins. IPsec: the new security standard for the Internet, Intranets, and virtual private networks. Prentice Hall Professional, 2003.

[3] Kumar, Sheo, Anil Kumar Gankotiya, and Kamlesh Dutta. "A comparative study of moodle with other e-learning systems." Electronics Computer Technology (ICECT), 2011 3rd International Conference on. Vol. 5. IEEE, 2011.

[4] Willis, C. . OWASP Broken Web Applications Project. 2010.

ABOUT THE AUTHORS

David Nuñez, PhD student, Department of Computer Science, Universidad de Málaga, Phone: +34 951952914, E-mail: dnunez@lcc.uma.es. Funded by the Junta de Andalucia FPI Research Programme.

Francisco Moyano, PhD student, Department of Computer Science, Universidad de Málaga, Phone: +34 951952914, E-mail: moyano@lcc.uma.es. Funded by the Spanish FPU Programme.

Ana Nieto, PhD student, Department of Computer Science, Universidad de Málaga, Phone: +34 951952914, E-mail: nieto@lcc.uma.es. Funded by the Spanish FPI Research Programme.

Juan J. Ortega, Assistant Professor, PhD, Department of Computer Science, Universidad de Málaga, Phone: +34 952134313, E-mail: juanjose@lcc.uma.es

Isaac Agudo, Associate Professor, Department of Computer Science, Universidad de Málaga, Phone: +34 952136315, E-mail: isaac@lcc.uma.es

Javier Lopez, Full Professor, Department of Computer Science, Universidad de Málaga, Phone: +34 9521313127, E-mail: jlm@lcc.uma.es