Internet Security Games as a Pedagogic Tool for Teaching Network Security

Suranjith Ariyapperuma[1], Amina Minhas[2]

Abstract - **This research investigates the suitability of online security games as a pedagogic tool, for teaching network security in an educational framework. Based on the advanced challenges they provide, we have selected security games offered by Next Generation Security. Our research is based on Network Security Principles, a core module in MSc Network Security at Anglia Polytechnic University. We compare two cohorts; both were given lectures and laboratory sessions. Only for the second group laboratory sessions were conducted by means of security games. We consider the game usage and views expressed by lecturers and students, to assess whether this method can be usefully incorporated in teaching specific sections of Information Security. Online and offline course feedback and interviews are used to assess the student experience. Quantitative and qualitative data gathered from this empirical study is analysed to derive conclusions. Advantages, discontents and educational concerns of this method are discussed. Deviation from current learning paradigms is addressed, in relation to the use of pure Internet based tools.**

Index Terms - Internet, Security, Games, Pedagogy

INTRODUCTION

The demand for trained network security professionals has increased exponentially due to the wide range of attacks on computer networks. We investigate the suitability of online security games as an alternative pedagogic tool to traditional labs, for teaching network security.

There are a wide range of Internet based labs available yet they are aimed for professional training [1]-[2] and are not used in academia. We evaluate their potential in conventional academic environments. Our research is based on Network Security Principles, a core module in MSc Network Security. We compare two cohorts from two academic years, following the above module. Both were given lectures and laboratory sessions. First group did not make use of online security games while laboratory sessions for the second group were conducted only by means of online games.

We consider the game usage and views expressed by lecturers and students, to assess whether this method could replace traditional labs in teaching specific sections of Information Security subject domain. An on-line survey was administered among the students. Online and offline course feedback and interviews are used to assess the student experience.

MSC IN INFORMATION SECURITY (MIS)

MIS is a comprehensive curriculum in Network Security offered by Anglia Polytechnic University UK [3] which allow students to use a range of learning resources in an integrated environment. In the design process of MIS our main target was to produce a good quality self-contained pedagogic program with easy access to the target audience. MIS address three facets of learning and teaching, the curriculum, practical skills and assessment.

The above considerations and restrictions such as time, cost and quality concerns involved in developing a curriculum persuaded us to consider adopting and integrating online security labs, which matched our defined course objectives. Furthermore the evolution of the labs according to the rapid evolution of the technologies underlying the course contents was a very important consideration for us. The lecturers already had a considerable amount of experience with similar games by Hackerslab [4].

NETWORK SECURITY PRINCIPLES

Network Security Principles is a core module in MIS. This mainly addresses penetration testing using a methodological approach and a selection of tools to exploit vulnerabilities at specific steps of the testing methodology. Further we discuss infrastructure protection, encompassing router and switch security, firewalls, intrusion detection systems and encryption technologies.

LABORATORY WORK

Laboratory work is a compulsory element of the pedagogy and is of gradually increasing complexity. For the first cohort lab sessions were conducted locally using a similar technique discussed by Helen [5] and Gregory [6]. Labs are linked to the learning objectives of the module. These labs included exploiting buffer overflows, password cracking, bypassing authentication mechanisms etc... For the second cohort lab sessions were conducted remotely using online security games. Remote labs are supported using web technology which provides a flexible remote access solution.

[1] Suranjith Priyandika Ariyapperuma, Senior Lecturer, Anglia Polytechnic University, England, s.p.ariyapperuma@apu.ac.uk
[2] Amina Minhas, Researcher, Anglia Polytechnic University, England, k.a.minhas@apu.ac.uk

NETWORK SECURITY GAMES

Security games are offered by organisations to educate and train network security professionals [7]. These games act as a legal means of testing security skills. Though these games are offered free of charge there is a lot of ongoing research and maintenance involved. Games involve a significant amount of research to solve problems presented at increasing levels of complexity and must be attempted in a sequential order.

Based on the advanced technical challenges they provide we selected internet based security games developed and maintained by Next Generation Security (NGSEC) [8]. This game has 11 levels, each requiring solving a challenge to obtain the authentication credentials. However brute forcing the authentication mechanism is not allowed.

A web browser is used to access the labs and HTTP protocol is used to transport lab content across networks to clients. Students required to use login credentials for authentication at the server. After completion of a level the challenge to the next level is sent by email. Further URLs, which point to external sites, are suggested to assist additional student research.

Setting up a conventional lab can be a good exercise [9]-[10] yet maintenance is a time consuming task depending on the hardware platforms used and the complexity of the labs. Further this would require onsite space, hardware, expertise for setting up [11] and ongoing maintenance. Since network security involves a complex combination of different operating systems and hardware platforms the time and cost involved in setting up and maintaining labs locally can be significant. This makes online labs a useful alternative as they incur no cost, and the availability of a wide range of labs maintained by dedicated professionals.

COURSE ASSESSMENT

The assessment of this program is being considered in three different, complementary, perspectives: students', academic staff and quality assurance team.

In the process of embedding the online labs in the MIS, assessment was one of the components that had to meet generic assessment requirements of the university at individual module level. Further we were concerned about the availability of lab solutions on the Internet; therefore we decided not to assess the students on the lab component but only to keep a progress indication which was complemented by a presentation by the student on the exploitation techniques used.

Only the final report based on a case study contributes to the final module mark. Each lab evaluates student's comprehensive knowledge on the corresponding learning objectives of the module. Completion of each lab determines the understanding of the module elements. This is an informal indication on the readiness to attempt the final report. Since the labs were not assessed, students were not required to undertake the labs at the university and were not invigilated.

The report is based on a comprehensive case study of a hypothetical network security architecture design, which includes Wide Area Networks as well as Local Area Networks. On par with the university regulations the reports are submitted anonymously by the students only using the student identification number. The reports are double marked for accuracy. Marks are compared with the access level achieved at the online labs. If online performance was significantly higher than the mark for the report, this can indicate possible errors in the marking process for the report. If the online achievement is significantly lower than the mark for the report, this can indicate the student has not attempted the report himself and does not meet the learning outcomes. In either case the student is invited for an interview.

COURSE DELIVERY PARADIGM AND STUDENTS

The pedagogic delivery model used for the second cohort is a paradigm shift from the traditional synchronous delivery which is classroom, laboratory and textbook based. The hybrid delivery model used combines both online and offline delivery. The online labs are accessed by students through the Internet. The offline component consists of lectures and tutorial support to complete the labs.

The students in the two sample cohorts from two academic years consisted of younger full-time students and mature part time students. Generally the mature part-time students are from a professional IT background. The sample cohorts included a minority of students from a non-technical background. Both groups consisted of technically competent students, some with professional experience in the IT industry, particularly in computer networking.

USAGE STATISTICS

Access was not requested to the original game servers maintained by NGSEC as they were accessed by a large number and this would create issues in isolating the relevant traffic for our experiment. For the purpose of usage analysis a proxy server was setup on the local network and students were requested to access the games through this. Usage statistics were collected for 73 days by means of analysing proxy server log files. This had a minimal effect since we were able to access all the usage statistics on the proxy server. This approach of connections through a proxy had an added advantage of not revealing sensitive information passed by our browser to the security portal.

The proxy is a Squid server [12] running on Linux.The log files for the year 2004 were analysed using Mach5 log analyser [13]. Generated statistics are used in assessing the usage of online labs. We specifically discuss, usage during the day, usage during the week, hits per day and server errors generated.

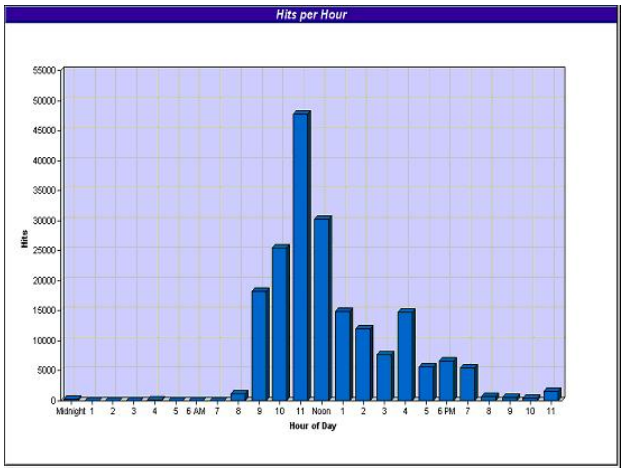

FIGURE 1
USAGE DURING THE DAY

Figure 1, Plots the number of visits against the hour of the day. Students preferred the morning and afternoon to study.

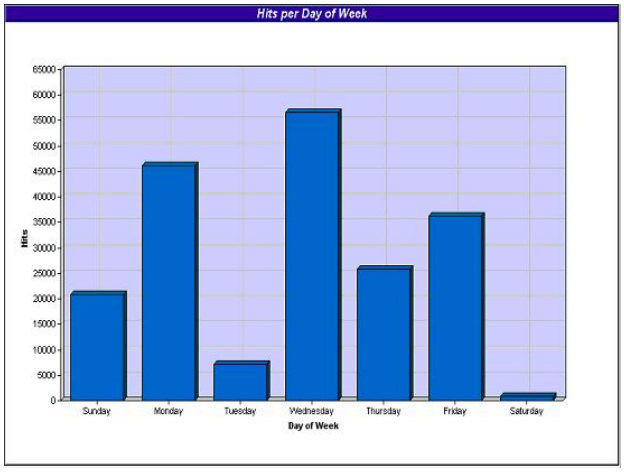

FIGURE 2
USAGE DURING THE WEEK

Figure 2, shows the usage during the week, minimal activity was recorded during the weekend. Figure 3, shows the number of hits per day, an exceptionally high amount of activity was recorded during the period before Christmas. The average number of users per day was 8 with 326 hits per day from each user. A total of 2.62 gigabytes were transferred during the experiment period.

The low percentage of server errors experienced by the users (0.008%) emphasized the reliability of online labs. A very low error percentage per request (1.8%), further proves the effectiveness of this method. 98.41% of these errors were due to unauthorised access attempts.

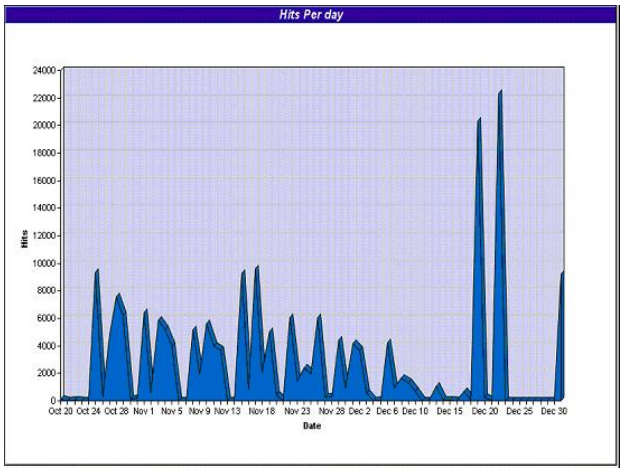

FIGURE 3
HITS PER DAY

INTERVIEWS AND QUESTIONER

Informal interviews were conducted among students to gather their experience. While a broad range of responses ranging from negative to positive were received from students, the main concern was adapting to the paradigm shift introduced by the online labs. However response was positive about 24/7 availability of labs and the support structure in place to complete them.

The questioner measured the student's desire and ability to participate in a course which used a hybrid pedagogic model, how many hours a week can be devoted to online training, and the advantages or disadvantages. These results were compared with usage statistics. Out of the 12 who responded to the survey, 96% have regular uninterrupted access to the Internet at home and work. Only 12% of the survey participants had experience with online labs before. During office hours, 68% of the respondents felt that they could devote one hour daily for training and 20% felt that they could devote two hours daily. After office hours, 32% of the respondents felt that they could devote three hours daily and 24% felt that they could devote two hours daily. Many of the participants felt that the weekends are a good time to undertake on-line study due to spare time yet the usage statistics contradicted this.

Pedagogy based on a hybrid model has several advantages and disadvantages. The two biggest advantages the survey participants gave were that the course is flexible and it allowed one to work at ones own pace and rhythm. Further it offered cost effective training. There were varied responses from the participants who had experienced online labs before as to when they attempted, which organisations offered the labs and the specific subject.

RESULTS

The overall results were purely based on the case study report. Lab work was not included as an assessment component. We

compare results from both cohorts. There was a significant improvement in the second group's results as they produced an extremely technical and accurate solution for the case study. Both cohorts consisted of relatively similar students. Both groups consisted of 15 students. The average for the first cohort was 53.3 with a standard deviation of 10.9. The average for the second cohort was 66.5 with a standard deviation of 13.8. A t-test confirms the improvements for samples with equal population variance (t-test probability of 0.0025). An F test on the sample variances indicates that they are from the same population, (alpha level of 0.005).

ANALYSIS OF MIS

The main concern for the quality assurance team was to monitor the participants' communicational behavior towards a set of pre-defined expectations. The overall quality of a course may be improved if a minimal threshold of specific, pre-defined, participation dynamics is accomplished. Each student must contact the lecturer to successfully overcome some basic operational procedures, such as obtaining access and authentication credentials for the lab servers. Another issue requiring special attention from the quality assurance team is the delay taken by an academic to answer a question conveyed online. This delay is one of the key issues in the student's perception of the quality of the course. The quality assurance teams monitor these events and guarantee that appropriate procedures and contingency measures are executed in a timely manner. Currently this is done manually and we propose a complete set of monitoring procedures to be defined with a course feedback system, including automatic and semi-automatic level tracking at the lab server. Further monitoring the lab completion time per student per lab is useful.

Currently accumulated experience has confirmed the importance of undertaking all the lab components by students even though they do not contribute to the final result. As this programme provides a postgraduate degree at MSc level and contain a significant amount of research, meetings between the academics and the student is considered to be an important element for the participants

CONCLUSION

This paper presents the results obtained regarding the integration of online security games in the MSc Information Security. The Internet security games presented in this paper were developed by NGSEC systems, these were adopted by us as an alternative to conventional labs and run embedded in MIS program during the year 2004.

The hybrid model adopted provides a good balance between pedagogic effectiveness and management flexibility. The pedagogic effectiveness is assessed by the success rate, the number of students attended and usage patterns of the online labs. Additionally, the outcome of online feedback by students largely confirms their satisfaction of the learning experience. Initially there was resistance from both staff and students towards the paradigm shift from traditional labs to Internet security games. Staff welcomed the introduction of vendor neutral material, but was concerned about the loss of flexibility in setting the labs as opposed to traditional labs.

Students were initially concerned about the new learning model, which prompted them to use online labs as opposed to traditional labs. But the ease of access, level of support from the staff and evolution of lab challenges were key factors in gaining students' confidence and helped them to grasp advanced concepts in an effective manner. Our survey found out that students would recommend this program of study.

Management flexibility is one of the strong points of this model, because it minimises the resources required to support the evolutionary development and release of labs. The constant and rapid evolution of underlying technologies requires periodical and, often, radical course and lab updates. This model accommodates these dynamic updates with limited resources and in a smaller time frame.

One of the key quality factors is the support provided by the academic staff, concerning both scientific adequacy and response time. To encourage the communication and social interaction among students during labs we encouraged the use of a Voice over Internet Protocol (VoIP) program, Skype [14] which enabled free communication via voice and chat. This significantly improved the interaction between participants.

The participant ages from young to mature confirmed the usefulness of this method for a broad audience. Students largely gave a high rank to the effectiveness of the online labs which supported their learning style. we can conclude that online labs and the amount of research involved to solve them contributed significantly to student's understanding.

Since the game servers are internationally accessible, belief is expressed that results are universal and the methodology can be applied universally. Further research can be conducted using the same methods, to evaluate other similar online games which address different subject content.

REFERENCES

[1] Microsoft, "Technet virtual lab: Security." [Online]. Available: http://www.microsoft.com/technet/traincert/virtuallab/security.mspx

[2] Netlab, "Remote labs by network development group inc." [Online]. Available: http://www.netdevgroup.com/index.htm

[3] APU, "Msc information security - course structure." [Online]. Available: www.isc.anglia.ac.uk/ics/msc/info struct.htm

[4] Hackerslab, "Hackerslab with free hacking zone." [Online]. Available: http://www.hackerslab.org/eorg/

[5] H. Ashman, "War games: Teaching web security hands-on," AusWeb2K, the Sixth Australian World Wide Web Conference. Southern Cross University Australia, 2000. [Online]. Available: http://ausweb.scu.edu.au/aw2k/papers/ashman/paper.html

[6] G. White, "Security across the curriculum:using computer security to teach computer science principles," 19th National Information Systems Security Conference Proceedings. National Security Agency. [Online]. Available: http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper003/seccur.pdf

[7] SecurityForest, "War games." [Online]. Available: http://www.securityforest.com/wiki/index.php/Category:LinkTree#War Games

[8] NGSEC, "Next generation security technologies." [Online]. Available:http://quiz.ngsec.com/

[9] M. Cook, "How to win at hacker wargames." [Online]. Available:http://www.happyhacker.org/wargame/howtob.shtml

[10] J. M. D. Hill, C. A. Carver, J. W. Humphries, and U. W. Pooch, "Using an isolated network laboratory to teach advanced networks and security," Proceedings of the 32nd SIGCSE Technical Symposium on Computer Science Education. Charlotte, North Carolina, February 21-25, 2001, pp. 36–40. [Online]. Available: citeseer.ist.psu.edu/hill01using.html

[11] W. Du and S. Narayanan, "Using minix to teach computer security courses," Department of Electrical Engineering and Computer Science Syracuse University. [Online]. Available: citeseer.ist.psu.edu/667321.html

[12] SquidProxy, "Squid proxy cache." [Online]. Available: http://www.squid-cache.org/

[13] Mach5, "Mach5 faststats analyzer." [Online]. Available: http://www.mach5.com/products/analyzer/index.php

[14] Skype, "Skype free internet telephony." [Online]. Available: http://www.skype.com/