

An Internet Role-game for the Laboratory of a Network Security Course

Luigi Catuogno
Dipartimento di Informatica ed Applicazioni
Universit\"a degli Studi di Salerno
Via Ponte Don Melillo
84089 Fisciano (SA)
ITALY
luicat@dia.unisa.it

Alfredo De Santis
Dipartimento di Informatica ed Applicazioni
Universit\"a degli Studi di Salerno
Via Ponte Don Melillo
84089 Fisciano (SA)
ITALY
ads@dia.unisa.it

ABSTRACT

Over the last few years, many universities and educational institutions have introduced computer security related courses to their degree programs. The majority of these courses feature intensive laboratory activity based on live experiments of attack and defense techniques by means of team games organized as “cyber-wars”. In this paper we argue that, although it is a useful tool for teaching and learning these techniques, the exercise paradigm does not cover all the aspects of security relating to a real-world scenario, with it not allowing students to experience the realistic needs of maintaining network services. In this paper we present the “role-game of the Internet” which was designed as part of the lab activity of our Network Security Course. In our game, instead of fighting against each other, student-teams had to cooperate in order to accomplish a list of business-like tasks over a simulation of the Internet while preserving the security and availability of featured network services.

Categories and Subject Descriptors
K.3.2 [Computers and education]: Information systems education

General Terms
Experimentation, Security

1. INTRODUCTION

Over the last few years, many universities and colleges have introduced system and network security related courses, which often have two parts. The first part consists of classical lectures which provide the fundamentals of cryptography and security as well as introduce related techniques and tools. While the second is carried out in the laboratory, allowing the students to work on “Hands-on” experiments and projects in order to experience, as well as put into practice, what they have learned. This activity is accomplished in an ad hoc laboratory that is equipped with computers as well as network hardware. Some of this laboratory activity focuses on live experiments of attack and defense techniques by means of team games organized as “cyber-wars”. For a few days, two or more teams of students set up their server to be defended and try to violate the computer of the other teams by using the techniques and the tools introduced in the lectures.

Nevertheless, computer networks are not arenas. The objectives of entities and people working on the Internet include sharing resources and data, providing and using applications and not just to set up networked systems running fictitious services, waiting for attacks. In the real world, Internet professionals set up services that have to work for a long time and be efficiently used as well as be carefully maintained. For these reasons we think that even though the cyber-war exercise paradigm gives an important educational contribution, it does not cover some relevant aspects of network security.

In fact, in many cases, vulnerabilities are not only due to bugs in the software as well as the operating system, but also to configuration errors, delays in system and software updates, inefficiency in system administration, lack of surveillance in the server farm as well as other aspects. In many cases, some services could work properly for a while, (or for a certain amount of handled data, workload or accesses) up until when a failure makes the system exploitable. Another important aspect that should be taken into account is that in the real world, the recovery of a computer that has been violated is a critical task. Systems cannot be re-installed from scratch but, configuration files, log files and user data should be carefully handled.

In order to understand what their security concerns are, students should be placed “in the shoes” of the administrator of a computer on the Internet. With this aim, we designed the “role-game of the Internet” which is described in Section 4. In this game, students form collaborative teams and participate in a simulation of the Internet in which each team plays the role of a different entity of the network (e.g., Corporations, ISPs, CA, domestic users, etc.) Each team has the responsibility of setting up and keeping secure and alive computers, services and applications related to its mission. Therefore, each team is required to accomplish a list of business tasks that we named job-orders. Each job-order is formed in a way that the teams need the effort of the other.
teams in order to complete it. This re-creates a (rather) realistic interaction between different entities of the network, since requests for services and products are aimed at achieving a given objective, instead of being just fictitious accesses. For example, a team playing as an Online Trader, in order to build its shop, could purchase hosting services provided by the ISP team, certification services provided by the CA team, etc. “Hands-on” experiments with attack techniques are also included in our game. Indeed, each participant individually plays the role of “adversary”, moving attacks to services and computers of the other teams.

In this paper we report our three-year experience in organizing the role-game as the laboratory activity for our Networks Security course. In Section 2 we present a brief discussion on related studies. In Section 3 we outline the goals we aim to achieve in our course. Thus, in Section 4 we introduce the role-game of the Internet as well as justify the approach. In Section 5 we stress the differences between the cyber-war approach and our role-game. In Section 6 we make some considerations about the experience and briefly report the students’ final feedback. Section 7 concludes the work.

2. RELATED WORK

The methodologies and tools to be used in teaching security related topics in computer science education have been the subject of wide discussion over the last few years. A brief description of several similar experiences in designing and implementing IT security courses by Universities and Colleges follows.

Studies reported in [1, 8, 2] stress the importance of holding practical experiences in a realistic laboratory that effectively simulates the real world. These studies describe the design and implementation of large labs equipped with professional hardware and ad hoc software solutions in order to support multiple experiments, activities and classes. Often the labs discussed in these studies are sponsored by network and computer corporations within their educational programs which frequently include product donation, advantageous purchase conditions, technical advice as well as other incentives.

This kind of joint activity between the university and the industry is very interesting and seems to be very attractive for students. However, we think that at least two considerations should be made. Firstly, laboratory activities have to be meticulously planned with the aim of educational goals in order to avoid students simply learning how to use lab equipment instead of security topics. For this reason, we believe that large and complex lab architectures could become distractive, with students paying more attention to studying hardware manuals rather than the teaching materials. Secondly, teaching materials, man-power and technical advice provided by the vendors of lab equipment should be carefully integrated with the course contents and in exercise activities, in order to avoid that skills needed by industry take the place of more wide and higher level knowledge. The reader can find an experience of “incorporating vendor-based training” into academic networking courses in [4].

Courses described in [6, 5, 11, 7, 9, 10], also deal with laboratory infrastructure implementation. However, they mainly focus on designing and planning the practical activities to be held during the course. Among these authors, structuring exercises as a cyber-war arena, seems to be the leading approach.

Conklin [3] introduces an annual Cyber defense competition held among several universities in the United States. Each team involved in the competition has to set up and administer a network of computers. It is asked to accomplish a list of business tasks on its network such as implementing and providing network services and products. In addition, each team has to defend its own network against attacks moved by the attackers team. There is a remarkable difference between this kind of competition and the “capture the flag” exercise. During the year, the students learned both attack and defense methods, but, in the competition they are not required simply to attack or defend some computers, they are also required to achieve business goals: providing some services guaranteeing their availability and security.

3. OUR COURSE

In this Section, we introduce the course of Networks Security II (NS2), giving an overview on its contents and the goal which we aim to achieve in this course.

The NS2 course is part of a degree course, it is scheduled over 12 weeks and is composed of twenty hours of lectures and twenty-eight hours of laboratory exercise. The courses of Network Security I, Operating Systems, and Computer Networks are prerequisites. The Networks Security I gives the students the fundamentals of cryptography, security theory and applications.

The lectures focused on important topics of computer security: technological solutions and improvements, state of art, discussions on cases of studies, ethical issues and seminars held by professionals and researchers involved in security related activities in the real world. The laboratory part of the course is absorbed by our role-game. The laboratory activities are not only limited to the hours scheduled for the course, we set-up an ad hoc free access laboratory for the purpose of the game.

3.1 Goals

In this course we aim to reach several important goals:

- allowing students to learn main security techniques and tools in order to build and defend secure systems which have to work for long time under realistic conditions in terms of user served, and amount of data handled.
- making students experienced of managing real services over the Internet, making choices, taking autonomous decisions in order to guarantee security and availability, taking care of data privacy and integrity;
- making students conscious about the importance of good work organization, job division, and accurate documentation of their work.

In Section 4 we present our role-game of the Internet, and the educational tool we designed in order to achieve these objectives.

3.2 The Laboratory

The equipment required for our simulation is not expensive. Each team was provided with a PC connected to an isolated LAN. No specific network hardware (routers, switches, wi-fi points, etc.) were provided. Students were allowed to freely choose which operating system and software to install.
4. THE ROLE GAME OF THE INTERNET

As outlined above, in our role game students form collaborative teams, playing entities of the Internet. Students have to manage realistic services which handle data coherent with a business-driven traffic. Therefore, in order to populate our simulation, we had to choose a set of roles which helped recreate a realistic reproduction of real business scenarios over the network.

In the three editions of our game, we chose to reproduce an e-commerce model where customers are allowed to purchase some goods through the web using credit cards. Thus, we introduced all network entities (roles) needed to summarize all transactions involved in this model.

Therefore, we created the following set of teams: The NIC team which took care of the network infrastructure (DNS, Name Authority, etc.), the CA team, which played a Certificate Issuer à la Verisign, one or more Internet Service Providers (ISP1, ISP2, ISP3, ...) which sold internet services such as web hosting, free e-mail, etc. In the first, two editions, we also formed the Attackers' team whose mission was to attack computers and services of other teams. In the third edition (Spring 2007), instead of creating an attackers' team, we chose to assign individual adversarial tasks to each participant, allowing all participants to experience being both attacker and defender.

Once the roles were stated, we formed the teams that had to play it. In a preliminary meeting, we presented the role to the participants, outlined the profile and the skills required for each team. Participants were allowed to freely choose the team to join.

The game was essentially composed of two phases. In the first phase, each team set-up its computers and services it provides. Participants were allowed to freely choose software, tools and technical solutions in order to achieve their mission. During this phase, teams held meetings in order to agree on common configuration issues (e.g., IP addressing, name conventions, etc.).

At the end of the first phase, the class had a meeting where each team presented the services it provided, describing and motivating its technical choices. They also illustrated any relevant aspects of the setup of its services. Moreover, each team had to release a complete technical documentation of its work and a customer guide of the services it provided.

The game of the Internet took place in the second phase which spanned over the rest of the semester. Actors of the simulation were: teams, individuals as well as the teachers who acted as game masters.

Participants played the game both as team members and individual players. For example, in the third edition of the game, we chose to secretly assign adversarial tasks to single participants instead of forming an attacker team. Other participants were unaware of the identity of attackers and of the nature of adversarial tasks. In this case, some participants lived as team member by day and as adversary by night.

Identities were characters who played a role in a job-order. For example, the identity Bob could be a customer who purchased something in one of web-shops maintained by another team.

Identities are defined by the masters and assigned to individuals in order to do some specific tasks (e.g., the master can ask a participant to submit a job-order as Bob) at any time. We used the identities to simulate the “network people”. Each identity had a mailbox, could open bank accounts, obtain a digital certificate, and so on.

As stated above, the lab exercises for the teams (and after for each participant) was to accomplish job-orders, i.e. business-like tasks which are submitted during the game. Within the simulation, job-orders could be submitted by the masters, by teams as well as individuals. Job-orders are the means we used to keep the simulation alive, since they were designed in a way that the destination team itself, had to issue new job-orders to any other team, in order to complete the requested task.

Since the design of job-orders is a crucial issue in our game, we roughly describe how we originate realistic transactions over the simulated network by job-orders. In this example, we assume that the simulation is populated by teams NIC, CA, ISP1 and ISP2 and that team ISP2 is maintaining an on-line payment system.

1. The master randomly chooses an individual and assigns the identity ACME Ltd. with the following job-order: build a web site and sell your product on-line

2. The identity ACME Ltd. issues several job-orders to proper teams in order to register the DNS domain acme.com, to create the mail account info@acme.com, to obtain a digital certificate and to apply for the on-line payment service.

3. ACME issues the following job-order to the ISP team: build the web site www.acme.com. This site has to be composed of a public area where customers can read information about the corporation and have access to the products catalogue as well as a private area where registered customers can purchase the products on-line paying by credit card. Information and the catalogue are provided in a separate file.

4. In addition, team ISP1 has to contact team ISP2 in order to enable on-line payments on the Acme Web site.

5. The master creates a bunch of identities and randomly assigns them to participants with the job-order: buy some ACME products. Some of these identities can be also assigned to attackers.

6. Once ACME Ltd. has its web site, newly created identities are enabled to submit to the ACME site a sequence of job-orders concerning several operations including: customer registration/deletion, goods purchase and payment.

Note that each operation by identities induces the team involved to ask for services from other teams in order to accomplish the task. In fact, for each private transaction, the web application of ISP has to check the identity of the issuing customer, that the credit card number does exist, that the digital certificate the customer presents during the transaction does exist and has not been revoked. The whole set of job-orders created in this process, produces realistic and coherent transactions over our simulated network.

Attackers are required to massively attack any component of the network, by means of both the usual attack methods (à la cyber-war) and by issuing malicious job-orders to the other teams.
Each attack has to be declared to the master before it is moved. When an attack has been moved, the attackers have to write down a detailed report which describes the used technique, the condition on top it is built and the results obtained. This report should also suggest to the victim any possible solution to the vulnerability discovered in its system by the attackers.

We developed a set of scripts and applications that make it possible to automatically issue large sets of several simple classes of job-orders (e.g., identity management, on-line purchase, etc.)

At the end of the Game, the whole class holds a final meeting in which each team presents a report where it describes the whole simulation and discusses all the tasks it accomplished, the goals achieved, the problems it encountered and how these have been solved. Another important topic of the final discussion is that the team evaluates and analyzes their own work, the collaboration with other teams, as well as makes critical considerations, stressing the positive and negative events experienced.

5. ROLE-GAME VERSUS CYBER-WAR

In this Section we briefly stress the differences between our approach and the cyber-war.

In the cyber-war exercises the emphasis is on intrusion and defense techniques. Students learn how operating systems and application bugs or incorrect settings (e.g., buffer-overflow, race conditions, dummy passwords, incorrect firewall rules, etc.) could be used by attackers to violate the computer. In the lab activities, students learn (by direct experience) how to collect information about possible vulnerabilities of their target and how to take advantage from such knowledge in developing attacks strategies. Furthermore, students learn how to correctly deploy defense tools including firewalls, IDSs etc. in order to face the same attack techniques they used against the “adversary”. This approach gives an essential contribute to the education of security experts, but, on the other hand, it does not cover some relevant aspects of network security, since the important technical skills it provides, are rather unlinked to the day to day management of the network.

A drawback of the cyber-war paradigm, is that participants adopt behaviors which are not suitable in the real world. We have given several examples which have justified our work.

- Often, during the cyber-war, students deploy paranoid defense approaches which, if adopted in reality, could make the system inefficient and its business services unavailable (e.g., waste of CPU time for packet filtering, huge log files, cumbersome user-interaction).

- Students pay too much attention to the initial installation of their system, but they do not take care in keeping an up-to-date operating system and libraries for the rest of the experience. Consequently, an initially secure system becomes exploitable a few weeks later, if a vulnerability of any software it runs has been discovered.

- Often, attacks are not unexpected because students know that any access to their computer hides an intrusion attempt, since there are not fair users on their systems.

- Students does not take care of the consequences of any received attack. Typically, they do not feature neither disaster-recovery policies nor data backup services. In fact, they do not have not user data to be protected.

Our role-game aims at dealing with these problems. Focusing on the business activity, and increasing the experience length up to the whole semester, we made it possible that the important issues and features of a networked computer appear in the lab experiences. In fact,

- giving business-like missions to the participants, induces them to mainly take care of keeping the services they offer secure and available, thinking of the learned techniques as a means to achieve their goals. Furthermore, in order to guarantee the availability of provided services for a long time, each team has to adopt a work organization so that each team member has its precise duty (e.g., system manager, application manager, R&D, ...)

- the simulation is kept alive by a certain level of network transactions which are not all due to intruders activities. Therefore, participant teams have to preserve the business traffic and distinguish it from the adversary’s

- the teams have to guarantee privacy, integrity and availability of the customer data and, in case of attack they should keep as brief as possible the off-line time of their computer.

6. OBSERVATIONS

During these three editions, we have found that the game substantially seems to reach the goals we stated.

In spite of difficulties in the early days, teams get the sense of the game and participants easily enter into their character. The participation and the contribution of students to the simulation has been enthusiastic and constant for the whole semester.

Although all the participants have a clear idea what they need in order to build a network service (e.g. hardware, software), they are often not conscious of which tasks and duties are required for the maintenance of this infrastructure. For several students, our game has been the first experience they ever had of being system administrators of a computer which hosts services available to third parties. In some cases, some participants did not worry that their computer could not be reached by customers for several days!

We observed that in all the teams, security concerns focused essentially in choosing stable releases of software and setting up firewalls. Participants paid a lot of attention to installing secure software (i.e., with no known bug) and in keeping the scan reports clean, but they did not take care of security of their policies and the software they developed. It is a common believed that Firewalls are the catch-all solution to almost all security threats. However, during the simulation, the majority of successful attacks were moved to firewalled hosts and were based on software bugs and misconfiguration of the operating system.

During the simulation, we held several meetings in which we discussed these behaviors and we agreed with students that it was mainly due to a lack of experience and that the game was useful in highlighting this problem.
In general, these observations and the participant feedback, convince us that our approach, is quite promising.

6.1 Participants feedback
At the end of the games we asked the participants to answer a set of questions about the aspects of their experience. Questions concerned the organization of the game, consideration of educational results as well as any criticisms and suggestions.

Students anonymously reported to be enthusiastic about playing the game. The majority thought that it was a good chance to apply the theoretical and practical concepts they had learned. Moreover, participants appreciate the whole organization of the simulation and in particular they considered periodical meetings an useful tool for achieving the educational goals of the simulation.

They also realized that the simulation proved that administering a computer on the network, and keeping it secure, raises several important problems which cannot be solved by just “installing a firewall” or “using cryptography”. The whole class agreed that the game has been one of the few occasions of realistic experience during the degree courses.

Students also agreed that the simulation contributed to making them conscious of the importance of being organized when working. On the other hand, many participants’ criticized the difficulty of students in setting up any form of organization and task subdivision. They reported that sometimes working in their team or, with other teams, wasted a considerable amount of time.

For each periodical meeting (as well as in the final meeting), each team had to write a report on the state of its work along with a brief presentation (20 minutes) to present their work to the rest of class. Students believed that this feature of the game helped a positive discussion in the team. Moreover, they believed that writing a good documentation of their work, and being able to effectively present it, is an important skill for their future career.

7. CONCLUSION
In this paper we report our three-year experience in holding an Internet role-game as laboratory exercises for the Network Security II course, held in Spring 2005, Spring 2006, Spring 2007.

In this game, teams of students acted as some of the actors in the Internet scenario. Each team had to set up its network services and cooperate with the others, in order to simulate the real-world interaction that makes the Internet alive and working. Teachers acted as users/customers issuing a set of job-orders in order to keep the simulation alive. An attackers team was also present. This game involved two teachers, and 13 students per year, and was conducted along the whole course in a free access dedicated laboratory.

The goal of this game is to allow students to learn about the main concerns about security in a real-world scenario, as well as experience managing issues of real and usable services over the Internet keeping them secure and alive. We argue that these important aspects are not completely captured by the cyber-war paradigm of lab activity, which seems to be, currently, the leading approach. Indeed, we found that although students have a good knowledge of main security tools (e.g., firewalls, network scanners), they are not completely conscious of what are the tasks that managing a network service requires. Another goal of this course is to stress the importance of working in a team and adopting an effective work organization, therefore we encouraged teams to implement a task subdivision as well as design policies and procedures in providing services.

We observed during the three editions of our game, which seems to validate our approach and show that topics we are focusing on are quite needed in the education of security professionals and IT professional at large and we believe that this kind of lab activity is a useful tool for reaching the goals of the course. On the other hand, students agree that the Internet role-game has been a satisfactory and useful experience. Participation of students is constant and intensive for the whole duration of the game.

8. REFERENCES