Computers & Education 69 (2013) 225–236

Contents lists available at ScienceDirect

Computers & Education

journal homepage: www.elsevier.com/locate/compedu

Design and evaluation of a learning environment to effectively provide network security skills

Ivan Marsa-Maestre*, Enrique de la Hoz, Jose Manuel Gimenez-Guzman, Miguel A. Lopez-Carmona

Computer Engineering Department, University of Alcala, Madrid, Spain

ARTICLE INFO

Article history:
Received 28 July 2012
Received in revised form
4 July 2013
Accepted 8 July 2013

Keywords:
Architectures for educational technology systems
Distributed learning environments
Interactive learning environments
Simulations
Teaching/learning strategies

ABSTRACT

Information system security and network security are topics of increasing importance in the information society. They are also topics where the adequate education of professionals requires the use of specific laboratory environments where the practical aspects of the discipline may be addressed. However, most approaches currently used are excessively static and lack the flexibility that the education requirements of security professionals demand. In this paper we present NEMESIS, a scenario generation framework for education on system and network security, which is based on virtualization technologies and has been designed to be open, distributed, modular, scalable and flexible. Finally, an example scenario is described and some results validating the benefits of its use in undergraduate computer security courses are shown.

1. Introduction

Information systems and networks play a paramount role in the contemporary societies. The degree of integration of these systems and networks in our daily lives is such that it is extremely difficult, if not impossible, to imagine our societies without them. Information systems are a key component in most government and enterprise structures. This dependency of the social infrastructures on the information systems supporting them makes societies as vulnerable as their underlying information systems are, which makes system and network protection a critical aspect (Shaw, Chen, Harris, & Huang, 2009).

To protect these systems and networks, there are two main categories of threats to take into account: physical threats and logical threats. If we analyze data from the last years, we can observe there has been a continuous increase in the number and severity of logical attacks to critical infrastructures (Cardenas, Roosta, & Sastry, 2009). This is specially true in the case of electronic attacks. For this reason, it is necessary to devote effective and efficient efforts to protect our infrastructures against these threats, and one of the critical requirements in order to achieve this is to be able to provide high quality education on information system and network security. This is not a new requirement, however. Since the 90s, different experts have recommended to strengthen the security-related subjects in the curriculums of network and computer science disciplines, pointing out that education on these matters is insufficient, and do not cover adequately the real needs (Yang et al., 2004).

Though there are different approaches to introduce system and network security in computer science courses, most of them distinguish two fundamental blocks: information security, where the main emphasis is put on the use of cryptographic techniques, and system security (Higgins, 1989). Specially in the latter case, one of the key requirements in order to provide a complete high-quality education is to have the adequate equipment. Due to the practical nature of the discipline, it is very difficult to address effective teaching on these topics without a lab environment where the practical aspects of the discipline may be studied (Lee, Uluagac, Fairbanks, & Copeland, 2011). However, even

* Corresponding author.
E-mail addresses: ivan.marsa@uah.es (I. Marsa-Maestre), enrique.delahoz@uah.es (E. de la Hoz), josem.gimenez@uah.es (J.M. Gimenez-Guzman), miguelangel.lopez@uah.es (M.A. Lopez-Carmona).

0360-1315/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compedu.2013.07.022

where there are resources to build this kind of labs, a common drawback is the difficulty to provide scenarios similar to real environments, which make students face challenges which are closer to those they would find in the real professional experience. In addition, due to the nature of the topics addressed in these subjects, system administrators are reluctant to the deployment of security labs in campus networks, unless they are isolated from the rest of the network. Therefore, most system security labs we can find are very limited, while most teachers would agree that the ideal case would be to provide the students with practical environments where they can interact with realistic systems using state-of-the-art technologies.

The design of realistic security labs is thus a challenge for the teachers of this kind of courses. In this line, our research aims to design security labs with realistic scenarios without negatively impacting the campus network performance, and in a modular and extensible way which allows the labs to be adapted to the rapid evolution of the discipline. This paper contributes to this goal in the following ways:

- We analyze the problem of teaching network and system security using scenarios, and we review the main existing approaches to teach this field (Section 3).
- We establish a set of requirements for a solution to generate and deploy realistic security scenarios (Section 4.1).
- We propose a hierarchical, modular model to define scenarios for network and system security in a flexible and extensible way (Section 4.2).
- We design an architecture based on virtual machines distributed among different physical machines, which allows to deploy complex scenarios in a scalable manner (Section 4.3).
- We provide a schema for scenario description based on templates and XML file descriptions, which allows for high expressiveness and flexibility in scenario definition (Section 4.4).
- We provide illustrative examples on the practical use of the proposed framework to teach system security (Section 5).

To validate the proposed framework, we provide a use case on its use as a support tool for network security education (Section 6), along with the discussion of the results obtained. Finally, the last section summarizes our contributions and sheds light on some future research lines.

2. Teaching network and system security

There are several traditional approaches to teach Network and System Security. Most courses we can find in universities differ both in the variety of topics covered and in the methodology used to address them. Regarding the contents of the courses, we can find basically three types: cryptography courses, system security courses and survey courses (Bishop, 1993). Cryptography courses are focused on the analysis, design and use of cryptographic mechanisms, and they usually rely heavily on mathematical foundations of cryptography, such as information theory, number theory and statistics. System security courses tend to draw apart from the foundations of cryptography (cryptography is seen here just as one more tool in the security professional toolbox) and focus on the design of secure information systems, usually covering the concepts of security threats, vulnerabilities and mechanisms to address them. Depending on the nature of the course, and usually of the context within the degree, there may be more emphasis in low-level technical details (such as vulnerability exploitation) or in high-level design principles (such as minimum privilege, segregation of duties or risk analysis). Finally, survey courses intend to give a general view of all the security-relevant topics, and thus cover both cryptography and network security in a more shallow way.

Regardless of the nature of the course from the point of view of its contents, there are different methodologies that have been traditionally used to teach information and network security (Khambari, Fairuz Iskandar Othman, Radzi Motsidi, & Faizal Abdollah, 2009; Sharma & Sefchek, 2007; Yurcik & Doss, 2001). The traditional lecture is probably the dominant approach we can find. Although this approach is probably justified in cryptography courses due to the need to understand the mathematical foundations of the discipline, it has the risk of becoming too descriptive and requiring so little involvement by the students that they may become too passive, and thus the learning process may not work adequately. Of course, techniques for making the lecture class more participative and appealing have been used, like providing real-life examples or in-class exercises. However, such an approach has the drawback of not incentivizing creative and lateral thinking, which are crucial elements in information system security.

Given the vastness of the security related topics, a growing tendency is to complement lectures with supplementary materials such as tutorials. There is a huge amount of freely available material on information security, which may be given to students as further readings and references in case they want to expand their understanding of a particular topic. This is usually of great help to keep the students motivated, since a broad offer of supplementary material increases the likelihood of finding a topic of particular interest to the student. However, most of this material is theoretical in nature, and even the practical material is very linearized (step-by-step how-to manuals, for instance), so there is still very little room for the students to develop discipline-related free thinking.

Finally, most current security courses in higher education complement the lecture approach with lab assignments. Lab assignments intend to put the student in contact with some of the topics in the discipline in a practical way. By having to apply the concepts learned in lectures to small practical projects, students not only interiorize concepts more easily, but also acquire a practical, hands-on view of security, which also helps to keep their motivation. The assignment may vary in difficulty and depth, from simple, highly-guided labs to small project-like assignments where students have to solve a more generally specified problem, such as securing a web server or designing a firewall architecture for a given fictitious corporation. Labs can be very motivating and rewarding for students, but it is very difficult to adjust their difficulty. Often small assignments are too mechanic to be a challenge, and complex projects may be frustrating and exceed the scope of the course (e.g. securing a web server would usually require to install the web server, which may be a time-consuming task not directly related to the course).

An alternative to have security labs which are motivational, instructive and affordable for the students is to devise a number of security-related scenarios which reproduce real problems of the discipline. These scenarios, if well designed and implemented, could allow students to face realistic assignments specifically tailored to suit their learning needs and capabilities, as has been successfully proven for other disciplines (Siddiqui, Khan, & Akhtar, 2008). In the following we discuss the requirements which such scenarios must have and propose an approach to facilitate their implementation.