An experiment teaching mode for an *Introduction to Information Security* course

Tao Zhang†, Mengjia Yin† & Yanxia Yang‡

Hubei Engineering University, Xiaogan, Hubei, People's Republic of China†
Wuhan University of Science and Technology City College, Wuhan, Hubei, People's Republic of China‡

ABSTRACT: An introduction to information security course is an important and practical one; it is typically reserved for upper division courses in computer science (CS) and computer information system (IS) programmes. The course delivered in an on-line environment poses challenges to the development of meaningful hands-on exercises for students. In this article, the authors present a summary of their study on experiment teaching in the *Introduction to Information Security* course, elaborate on the target of experiment teaching, analyse the experimental content and describe the experiment teaching process. The experiments undertaken have proved successful in enhancing the learning experiences of undergraduate students in the area of information security. At the same time, they provided the teachers with a good platform for information security research experiments.

INTRODUCTION

With the rapid development of the social economy, informatisation provides new development opportunities, but at the same time it also brings serious challenges to economic development, national security, social stability, etc. Due to the swift, professional and appropriate action provided in response to information security risks and the parallel development of information security industry with information security professionals capable of preventing all kinds of information disclosure and minimising risks, hacker attacks and inappropriate on-line behaviour are relatively scarce and well managed.

Conservative estimates regarding the informatisation spread in China indicate that the demand for all kinds of information security professionals are as high as over 100,000 per year. However, China can produce only 50,000 high level information security professionals per year, which causes an especially big gap between the demand and supply of those professionals. [1].

It appears that the solution to this problem lies in building up an information security talent training system suited to the needs of society and further developing those information security professionals, especially, the ones that have an aptitude for identifying and solving serious security risks.

Huiming Yu developed a course module named *Introduction to Writing Secure Code* [2]. This module covers computer security concepts, secure code, safe programming practices; and it includes laboratory exercises. This module could be taught in first-year freshman and second-year sophomore classes of software engineering, computer science and information technology.

Markham argues that information security is an important topic that should be introduced early and offered throughout the undergraduate curriculum [3]. Security is pervasive in all disciplines of computer related areas and an early introduction would not only accentuate its importance, but also create an entry point for the proper skill development. Rather than labelling security as only one of many specialised areas, it should be treated as a common area for university courses and incorporated into all relevant subjects as increased worldwide connectivity enhances the need for security.

The Swedish University's Information Security Group stated that nowadays students usually have an extensive experience of using a computer well before they begin their university studies. If students are to become responsible computer users, they must learn about computer security in the school system. The Group has conducted a preliminary study of the current computer security situation and developed a questionnaire on the degree of technology and security knowledge with a view to introducing computer use and computer security into the school system [4].

Information security is part of the computer science discipline, and can still be regarded as an emerging discipline. It involves communication, computer science, informatics, mathematics, and many other disciplines. The main research scope involves all aspects of the computer and network security.

The *Introduction to Information Security* course, which is the main focus of this article, presents the principles and mechanisms of computer resource management and contains many abstract concepts and algorithms. Students feel that the content of the course is elusive and are not very confident when they have to learn for the course. Therefore, it appears crucial to deploy a teaching method that would enable students to achieve better outcomes in a less stressful way. Experiment teaching is one of such methods. In experiment teaching, students conduct experiments related to real problems in order to solve them. They start from abstract theories, but move quickly to real life problems and through the application of the learned theories attempt to solve these problems. This method of teaching cultivates students' ability for knowledge application and innovation, and for the deep understanding of the actual problem.

In recent years, the authors of this article, based on different teaching objectives and teaching requirements, have designed several means in which students could conduct experimental projects. The authors have made some fruitful exploration of the teaching practice in the introduction to information security course and set up an experiment teaching system to improve the practical application ability of students.

CONSTRUCTION PRINCIPLES OF INFORMATION SECURITY LABORATORY

An information security laboratory is required for experiment teaching and task practising in information security, network system management, computer applications and other professional information security courses. At the same time, it could provide good support for research and professional skill certification training. The setting up of the laboratory should conform to the overall trends in the latest technology, and the following principles should be considered during the formative stage:

Advanced and Forward-looking

The authors choose advanced technology experimental equipment to better adapt to new directions in teaching, scientific research and practice. The experiment teaching, technology development, innovation and research application should be organically integrated as this integration creates synergies for teaching, scientific research and also students' employment prospects.

Scalability and Flexibility

With new trends and developments in information security technology, updating the content of the laboratory must be timely and new experimental teaching equipment must be added, in accordance with the developments. However, if the laboratory is established in line with the current trends, there may not be a great need to update the equipment and network architecture for some time; the experimental management platform system should also be able to be managed and controled.

Security and Controllability

As some experiments in the laboratory assume certain risks, which could manifest as real, though inadvertent attacks and cause damage, the teacher must guide students and focus their attention on network control. More specifically, the laboratory internal networks and the Internet must be completely isolated. Only through the complete isolation of the internal- and the external network, students and teachers can effectively detect attacks on the laboratory's internal network data and spot unusual behaviour.

Teachers occasionally need to check and record the network's communication data, monitor real-data and audit attacks that had happened. The research data involved in the experiments have to be closely protected, under no circumstances should they be allowed to leak. All these measures have to ensure that the security of information security experiment environment is safe and intact.

THE FUNCTION OF INFORMATION SECURITY LABORATORY

The security laboratory is an important support platform for practice teaching, scientific research, application of technological developments, and professional and technical training [5]. The laboratory performs the following three service functions:

Practice Teaching

The laboratory is a practice teaching place for information security, network system management and other professional courses. Students, through the experimental teaching system, complete the relevant experiment and training tasks. Teachers use tools to create courseware resources, demonstrate experimental operation processes, prepare downloads for students to study in the teaching resource network, and also provide the Internet environment for students to access information.

The Study of Science

In regard to research needs and functions, the laboratory provides a good experimental environment for teachers that are engaged in research. The teachers can complete their investigations, development and application work on the network and in the area of information security, which helps to rapidly promote the teaching by those teachers and their research achievements. At the same time, the laboratory provides an infrastructure for the information security discipline and for making plans for a talent training scheme.

THE GOAL OF EXPERIMENT TEACHING

Information security courses delivered in an on-line environment pose challenges to the development of meaningful hands-on exercises for students [6]. The authors of this article argue that the introduction to the information security course is indispensable and has two main goals:

Help students to understand basic concepts, principle and mechanisms of information security: the introduction to information security course includes many abstract basic concepts, such as access control, security model and system reliability; and it also contains more complex algorithms and mechanisms, such as symmetric encryption and authentication [7]. For undergraduate students, this knowledge is relatively difficult to understand and absorb. The experiment teaching of the course should expose students to real processes of the information security internal implementation and, thereby, help them better understand basic concepts, principles and mechanisms of information security.

Cultivate students' ability to apply the acquired knowledge in information security: the course content covers the core of computer system software, and future professionals that will be engaged in computer industry need to grasp the principles of this knowledge. Because their roles could be different in future employment, they will face different problems and will need to have the ability to apply the learned knowledge according to a specific situation. The experiment teaching of the course must accommodate the differences in student learning styles and characteristics, so that all of them are adequately prepared for success in the job market.

THE DESIGN OF EXPERIMENT TEACHING

In accordance with the teaching goals, the authors have designed a number of experiment items. From the perspective of safety technology, the content covers host safety, the authentic perspective of action, access control, firewalls, intrusion detection, etc. From the engineering and technical perspective, the content covers computer systems, networks, computer communication, information databases and Web site security, and multi-disciplinary engineering technical knowledge. Considering the background knowledge and experience of students, the arrangement of the experimental project has to proceed from simple to difficult. Students have to rely on the guidance by teachers, but design independently [8].

The basic verification experiment directly runs on the simulation software, where the experiment's results can be viewed. The experiment mainly cultivates students' basic skills, ensuring that they can adapt to the basic requirement of information security society [9]. This experiment comprises a cryptography experiment, an operating system security experiment and a network scanning experiment.

The open experiment's emphasis is on cultivating students' comprehensive ability to apply theoretical knowledge and enhance their ability to design, as well as their overall understanding of applications in concrete practice. This experiment includes PGP, Skynet firewall configuration and the use of intrusion detection systems.

The research innovation experiment cultivates students' innovative consciousness and team cooperation spirit, improves their ability for understanding information security technology issues and challenges, and develops their comprehensive design ability [10]. This part of the experiment is highly demanding, and students should not only possess solid knowledge of information security theory, but should have a certain programming ability.

Teachers can require that students complete the design and implementation of a given function, according to innovative ideas, but being guided by the teachers. Specific tests, such as testing and design of network access behaviour, design and realisation of P2P file security transmission platform, etc, can be derived from teachers' research projects and form the students' independent research topics.

EFFECTIVE USE OF VARIOUS EXPERIMENT TEACHING METHODS

The development of computer science and technology changes the way in which society functions. It is therefore crucial to strengthen practical teaching to ensure that students adapt to the changing needs of society. Teachers should seriously and comprehensively consider the characteristics of information security talents demonstrated by students, support their development, and pay particular attention to the application and practical ability. The task-driven teaching method should be used, where analysis, resolution, elaboration and summary, knowledge acquisition and skill exercise take place and are blended among the process parts, through the process of introduction to a specific task.

Changes to the traditional teaching mode of *the teacher as the centre, teaching material as the centre and cramming education* to the mode of *the student as the centre, ability as the goal, students' active participation, learning autonomy, cooperation, exploration and innovation*, can significantly improve the process of teaching and learning, yield better outcomes and adequately prepare students for the job market. Conducting a series of student extracurricular activities in science and technology, social practice and technology competitions encourages students to engage in research and innovation activities, as well as enriches and perfects the teaching system [11].

Also, when students encounter all kinds of information security problems using computers and networks, their problem interpretation and resolution can effectively improve their interest in learning [12]. On the course's Web site, teachers need to provide course sharing resources, such as screen videos that guide students' autonomous learning. It is also important to realise the hierarchical teaching approach to meet the needs of a diverse cohort of students. A variety of flexibly used teaching methods and modes allows students' active participation in the experiment teaching.

CONCLUSIONS

Through the design of a multi-level experiment system, students can carry out experiments at different levels and directions, and discuss and analyse the experimental process and data. This system helps students better understand or even master theoretical knowledge and improves their practical abilities. At the same time, the system provides the teachers engaged in network and information security research with a good platform for experiments.

In recent years, this teaching method produced good results, but there are still some problems that require further exploration and study. In regard to the experiment teaching content, teachers need to update it constantly and present the latest knowledge to students; and in regard to the experiment teaching's implementation, teachers need to further enhance students' interaction in the laboratory and timely adjust the experiment according to technological changes.

ACKNOWLEDGMENTS

This work is supported by the Hubei Engineering University Teaching Reform Project (No.2014B07).

REFERENCES

1. Tang, H., Meng, F., Sun, C., Han, L. and Qu, X., Construction of network and information security experiment teaching platform. *Experimental Technol. and Manage.*, 27, **9**, 118-120 (2010).
2. Yu, H., Jones, N., Bullock, G. and Yuan, X.H.Y., Teaching secure software engineering: writing secure code. *Proc. 2011 7th Central and Eastern European Software Engng. Conf.* (2011).
3. Markham, S.A. Expanding security awareness in introductory computer science courses, *Proc. 2009 Information Security Curriculum Develop. Annual Conf.*, 27-3 1 (2009).
4. Wenngren, G., The SUSEC school project: introducing computer security to teachers and pupils. *Proc. IFIP Advances in Infor. and Communication Technol.*, 57, 55-69 (2001).
5. Zeng, X. and Wu, M., Reflections on and practice of construction of training workshops at technical colleges. *Research and Exploration in Laboratory*, 30, **12**, 217-221 (2011).
6. Bhagyavati, Laboratory exercises in online information assurance courses. *ACM J. on Educational Resources in Computing*, 6, **4** (2006).
7. Huang, H., Chen, S. and Huang, C., Computer teaching based on experiments using a virtualisation platform. *World Trans. on Engng. and Technol. Educ.*, 11, **4**, 527-531 (2013).
8. Liu, J. and Lu, Y., Design and research of introduction to information security course experiment teaching. *Experimental Technol. and Manage.*, 28, **1**, 153-155 (2011).
9. Zhang, H. and Wang, L., *Information Security Comprehensive Experiment Tutorial*. Wuhan: Wuhan University Press (2006).
10. Hou, Z., Xu, J. and Zhu, X., On teaching and practice of information security specialty. *J. of Hefei University of Technol. (Social Sciences)*, 22, **3**, 51-53 (2008).
11. Zhang, T. and Yin, M., Applying humanistic values to computer practical teaching for quality education. *World Trans. on Engng. and Technol. Educ.*, 12, **2**, 298-301 (2014).
12. Fan, L., Methods for improving the professional level of students majoring in information and computer science. *World Trans. on Engng. and Technol. Educ.*, 12, **1**, 122-126 (2014).