

Exploration of teaching reform of network security experiment course under the background of emerging engineering education

Xiaoming Ye^{1,2,*}, Zhibo Du^{1,2}, and Gang Gan^{1,2}

¹Chengdu University of Information Technology, School of Cybersecurity, 610225, Chengdu, China

²Advanced Cryptography and System Security Key Laboratory of Sichuan Province, 610225, Chengdu, China

Abstract. Given the practical needs of network security professionals against the background of emerging engineering and guided by principles of cultivating stronger innovation ability and frontier problem-solving ability, this paper, a case study of a network security experiment course, proposes to build an open training platform with multidisciplinary cooperation and multi-party participation in order to provide solutions to existing problems. It attempts to enhance school-enterprise cooperation and jointly determine the complex engineering problems of network security. Following the pattern of the post-role competency, typical engineering problems, and hierarchical experimental projects, this paper explores the teaching reform of a network security experiment course by realizing individualized and differentiated evaluation of the course's teaching effectiveness.

1 Introduction

It is crucial to develop high-quality, compound emerging engineering talents in the new environment and circumstances who are in line with the development of national strategic emerging technologies, who can handle the demands of building new infrastructure and developing interdisciplinary collaborative innovations, and who possess both cutting-edge theoretical knowledge and comprehensive application ability[1][2]. There is an urgent need for the assistance of diverse and excellent engineering and technology specialists during this crucial time of new scientific and technological revolution and industrial change, particularly since China's new economy is developing quickly[3].

Students majoring in network security are required to meet new standards based on the evolving engineering background[4]. Electronic information technology, the digital economy, and network security all require a lot of technical abilities to develop[5]. As a result, this paper investigates and establishes a teaching reform model of student immersive participation, scientific research innovation challenge, and whole-process project progression, followed by thorough application in the network security experiment course, based on the practical needs of network security professionals in the context of emerging

* Corresponding author: yexm@cuit.edu.cn

engineering and guided by the goal of cultivating stronger innovation ability and frontier problem-solving ability.

2 Analysis the teaching of experiment course

The network security experiment course aims to enable students of information security majors to apply knowledge from multiple courses to solve practical network security problems after taking elementary theoretical courses in computer network, operating system, program design, cryptography, information security architecture, and OSI network protocol analysis. It is a course that thoroughly combines theory and practice in the information security major's training program and curriculum structure.

This course covers the full process of security data collection, data preparation, data analysis, and solution creation, which includes numerous abstract ideas, models, and algorithms [6]. As a core engineering practice course for junior students majoring in information security, it plays an important transitional role. On the one hand, it focuses on developing students' abilities to solve difficult engineering issues based on basic theoretical knowledge. On the other hand, it lays the foundation for a comprehensive practice course and graduation design that come in the fourth year [7] [8]. Consequently, the current network security experiment course must be improved in the following three ways.

1) Cross-integration of teaching contents and the construction of an engineering scenario experiential teaching and students' independent participation

Emerging engineering focuses on developing the ability to address complex engineering challenges. However, in the real world of teaching, teachers lack practical expertise in project technology development and operation management. Because of this, only a small part of the engineering scenario can be found in the open modules of the enterprises, and the majority of the projects are out of date and lack critical technical modules [9]. As a result, teachers have difficulty keeping up with the times in terms of project design and updating, as well as accurately understanding and grasping the new characteristics of complicated engineering challenges, causing them to lose touch with reality.

2) Experiential teaching and students' independent participation

At the moment, teachers continue to use traditional classroom teaching methods rather than student-centered research-based teaching approaches [10]. There are several issues: the classroom environment is dull and boring; the teaching effect is polarized; a small number of active students can fully understand the network security framework through independent learning; most students only aim to pass course exams; and they complete experiments solely on the basis of experimental instruction without taking the initiative to think critically and creatively.

3) Objective and diversified teaching evaluation and overall feedback of students' ability

Curriculum assessment continues to rely on conventional evaluation methods. There is no professional method for evaluating the effectiveness of educational courses. Particularly lacking in teaching effectiveness evaluation is a breakdown of the students' ability index into its component parts [11].

3 Exploration of teaching reform

As for network security experiment course reform in the context of emerging engineering, efforts should focus on optimizing and improving teaching contents and methodologies, as well as completing process assessment methods.

3.1 Design of course teaching contents

We can address difficult network security engineering problems by collaborating with schools and businesses. First, it should conform to the development of cutting-edge technology, consider talent demands for the development of strategic emerging industries, and emphasize that graduates can effectively meet the requirements for the development of emerging industries in terms of both theoretical knowledge and engineering skills. As a result, reform should focus on professional curriculum systems to build an open training platform with multidisciplinary collaboration and joint participation as well as encourage school-enterprise collaboration to jointly determine the complicated engineering problems of network security.

The course's top-level design should emphasize practical network security engineering scenarios, incorporate the post-role and competency model, and create hierarchical elementary, intermediate, and advanced-level engineering challenges by setting professional scenarios by varying levels. In addition, the experiment must be paired with corresponding fundamental training units, comprehensive analysis projects, challenging research projects, and competitions in order to form the project chain course mode of fundamental experiment mainline, node-based innovation experiment, and project-based innovation experiment. Using the function of an information security management engineer as an example to design the course content, as illustrated in Figure 1.

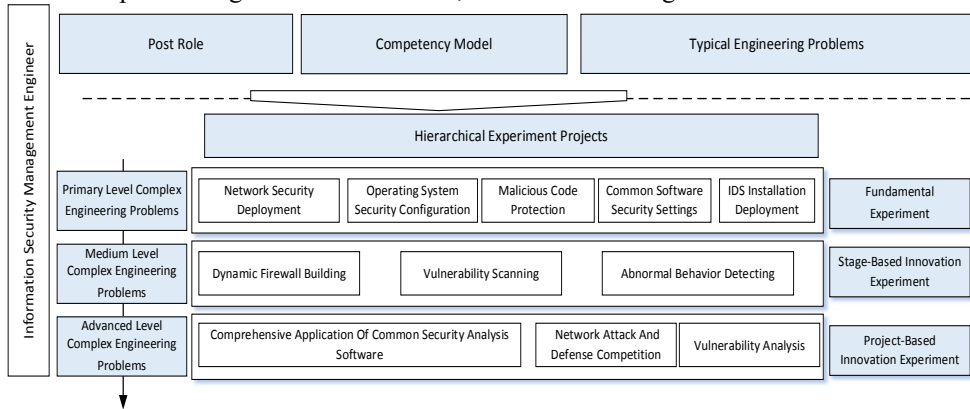


Fig. 1. A case of network security experiment design.

In the network security experiment course, teachers construct a library of innovative projects. Cooperative businesses and frontline educators determine the innovation content of complex network security engineering problems jointly. The project environment should progress from simple to complex. Projects must have a clear sequential association, along with stated research objectives and technical evaluation indicators. The source of the project is closely related to the enterprise innovation practice. Project practice can be directly applied to scientific research or competitions, such as the Challenge Cup, the national college student information security challenge, and the college student computing competition, among others.

3.2 Course teaching reform

Implement the above-mentioned designed teaching content and further optimize teaching methods. This paper proposes combining the content of experiments, applying simulation technology, and developing an online simulation experiment platform to manage students' practice processes dynamically [12-13].

1) Teachers employ cloud desktop technology to manage experimental equipment resources in a centralized manner, allowing students to complete the experiment procedure independently.

2) To effectively accomplish the flipped classroom effect, teachers track and record students' experimental data. Meanwhile, during the experiment, teachers and students can communicate in real time.

3) The simulation experiment platform based on the B/S framework allows students to perform experiments while professors dynamically monitor the process, breaking the constraint of time and space for teaching and learning.

4) To increase the teaching effect of the network security experiment course, each group of students can record and share videos of their experiment findings with their peers. Students have been tremendously motivated to participate in online classes as a result of such contact. Several groups have created videos to share with the class. Students can truly become devoted and thrilled about pursuing solutions in this manner. It has played a vital role in education and has boosted students' information absorption rates.

3.3 Improvement of teaching assessment

Regarding course evaluation, we have highlighted student-centered evaluation methods that are also in line with the teaching process and lesson plans. Additionally, a professional course teaching effectiveness evaluation method should concentrate on the three-dimensional views of profession, accomplishment, and practice, as illustrated in Figure 2.

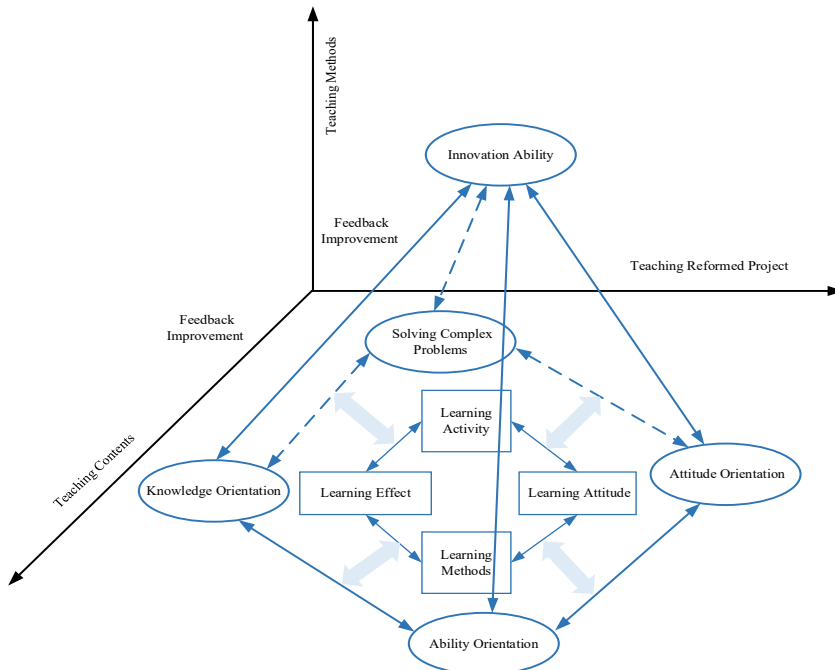


Fig. 2. Teaching effectiveness evaluation system.

The course teaching effectiveness evaluation method can operate in the two modes listed below. On the one hand, it emphasizes the improvement of students' professional quality and professional skills through course teaching and achieves the effect of feedback and improvement closed loops during the teaching and learning process so as to enhance the quality of course teaching; on the other hand, teachers can conduct horizontal and

vertical comparative analyses of project completion indexes of the same grade in different years to improve course teaching content, experiment design, and assessment methods.

4 Conclusion

This study, which is grounded in emerging engineering and makes reference to the network security business and other associated emerging industries, focuses on three key issues: teaching content, teaching methodology, and teaching assessment. This study examines the teaching reform of the integration of emerging engineering thinking and network security experiment course, keeping students at the center and guided by the principle of developing greater innovation capacity and frontier problem-solving ability.

Following the pattern of the post-role, competency, typical engineering problems, and hierarchical experimental projects, this paper designs and expands the open training platform with multidisciplinary cooperation and multi-party participation while focusing on the professional curriculum system. It also attempts to improve school-enterprise cooperation so that they can jointly determine the complex engineering problems of network security. This paper aims to enhance students' ability in fundamental theory, engineering practice, and innovative application at the same time so that they can gradually adapt to the constant development and changes of network security technology in the future by continuously improving the teaching content, experiment projects, and teaching methods of the network security experiment course.

This work is supported by Teaching Research and Reform Project of Chengdu University of Information Technology (No. JYJG2022126, JYJG2023083), College Students' Innovative Entrepreneurial Training Plan Program of Chengdu University of Information Technology (No. 20201062125, 202110621224, 202110621225), the Sichuan Philosophy and Social Sciences (No. SC21B034), and the Sichuan Science and Technology Program (No. 23ZDYF0380).

References

1. M. Ye, L. Sun and J. Shen, *EEIT*, 62-65 (2022)
2. H. Yan, H. Ao and Z. Chen, *EEIT*, 54-57 (2022)
3. H. Zhang and F. Zhang, *GCRAIT*, 381-383 (2022)
4. Z. Ting, *AEECA*, 1104-1108 (2022)
5. P. Xia, *IWCMC*, 199-203 (2020)
6. W.P. Chen, Y.X. Lin, Z.Y. Ren, D. Shen, *Comput. Appl. Eng. Educ*, 114-129 (2021)
7. M. Luo, Z.Cheng, J. Shen, *HSMET*, 336-341 (2019)
8. X. Yang, *CSIA*, 928, 1432-1436 (2019)
9. D.Y. Baskakova, O.Y. Belash, S.O. Shaposhnikov, T and QM and IS, 783-787 (2021)
10. L. Xu, S. Fang, L. Hobbs, *Int. J. Sci. Math. Educ*, 667-689 (2023)
11. M. Tian, G. Lu, L.Li, H. Yin, *Front. Psychol.* 12, 2139 (2021)
12. Y. Wang, H. Li, *ITMS*,34, 891-893 (2015)
13. J. Zhang, *ICMSOA* ,2173, 12013-12015 (2022)