Project-Based Cyber Security Course Teaching Based on Digital Training Platform

Yang Li and Wenting Li(✉)

College of Computer and Information Engineering, Guizhou University of Commerce, Guiyang, China

wendyworkmail@163.com

Abstract. As cyber security issues are becoming obvious around the world, the training of cyber security professionals is particularly important. Educators are trying to find effective teaching ways for cyber security education. In order to help students develop both theoretical and practical abilities, project-based teaching mode is used in cyber security course. During the teaching process, teachers match chapters with the components of the real project, use project to introduce theories, and make project design tasks for students. During the semester, students should complete six module design task and a whole project design scheme at the final. There are two digital platforms, one for basic experiments and the other for design tasks. This teaching mode can help to achieve the integration of theoretical knowledge and engineering practice. It also helps students make a good habit of study.

Keywords: project-based · cybersecurity course · digital platform · modular teaching · design task

1 Introduction

Internet technology has developed rapidly in recent years. The cyber security problems become obvious. Therefore, many universities pay great attention to developing outstanding cyber security talents. Educators are also constantly exploring the teaching methods of cyber security courses and trying to make innovations.

Cyber Security mechanism is the practice of protecting the network, data storage, programs and the overall systems from potential cyber attacks [1]. Cyber security is a course based on computer cryptography, which studies encryption algorithms, cyber security protocols, firewalls, intrusion detection and other technologies. The teaching goal of this course is to enable students to learn about the theory of cryptography, understand the principles of computer networks and system security configuration and know about security vulnerabilities, cyber attack and prevention technologies [2]. Cyeber security students should also be familiar with network security protocols, and have strong theoretical and practical abilities of cyber security. Cyber security course plays a core role in major of network engineering. The traditional teaching way of cyber security course seems boring. It contains many concepts, which makes students difficult to understand.

X. Yuan et al. (Eds.): ICEKIM 2023, AHCS 13, pp. 763–772, 2023.
https://doi.org/10.2991/978-94-6463-172-2_80

Students would have no interest, and do not understand the practical application of cyber security technologies [3].

In recent years, teachers in colleges and universities are also constantly exploring the teaching methods of cyber security courses, such as using the “competition to promote learning” model [4] to improve students’ interest in learning, using the “flipped classroom” [5] teaching method to strengthen students’ learning initiative, and using virtual simulation technology [6] to cultivate students’ practical ability. Although the existing teaching mode of cyber security course has been able to give consideration to both theory and practice, the content of course teaching is still separated from the real engineering projects. In this teaching mode, students mostly focus on principle experiments and verification experiments in practical learning after learning theoretical knowledge. They still do not know how to use cyber security technology in real projects. This kind of teaching method does not achieve the real integration of theory and practice.

In order to achieve this goal, the teaching of cyber security course must be carried out under real engineering projects. Based on the "secondary safety protection project of Guiyang smart energy system”, which is a real engineering project about cyber security, the project-based teaching mode is used in class of cyber security course in Guizhou university of Commerce. The course content was deconstructed, and the theoretical knowledge of each chapter corresponds to each part of the project one by one. To solve the problem of separation between course teaching and engineering practice, real engineering projects were used in the classroom teaching. The digital experimental platform is used to carry out the basic and extended experiments of the course, and finally complete the overall project design scheme. The engineering project scheme is used to help students understand the practical application of cyber security technology in the project, so as to achieve the integration of theoretical knowledge and engineering practice.

2 Combination of Real Engineering Project and Course

In the process of project-based teaching, teachers can combine projects from their familiar industrial fields for teaching, so as to achieve better teaching results. In this research, based on the familiarity with the energy field, the educator used the cyber security protection scheme of smart energy system as a main case. So that students can understand the cyber security problems faced by the energy system in the course of learning. It also makes students realize that as a cyber security professional, they can also play an important role to do something in different fields, such as to protect energy systems. Through the implementation of this research, the researchers want to explore the way of project-based teaching of cyber security courses, and summarize the teaching mode of training professionals in the field of cyberspace security.

Based on the “Guiyang Smart Energy System Secondary Security Protection Scheme”, the main knowledge points of cyber security course was divided into six modules, corresponding to the six major components involved in the secondary security protection scheme (as shown in Table 1). Case-based teaching, discussion-based teaching and other teaching methods are used in class to help to match the chapters with the components of the engineering project, so as to achieve the integration of theoretical knowledge and engineering practice. Students can deepen their understanding

Table 1. Module division of curriculum knowledge system

Module	Knowledge Points and Chapters	Components of Project
1	Chapter 2 ~ 3: Data Encryption Algorithms	Longitudinal Encryption Device
2	Chapter 4: Data Authentication and Signature	Encryption Authentication Gateway
3	Chapter 5: Cyber Security Protocols	Grid Connection Interface Device
4	Chapter 6 ~ 7: Wireless Security and Cloud Security	Wireless Communication Module
5	Chapter 8: Network Perimeter Security	Forward And Reverse Isolator
6	Chapter 9 ~ 10: Intrusion Detection	Safety Monitoring and Anti Permeability System

of theoretical knowledge through engineering cases. And then they use the theoretical knowledge to solve new engineering problems and complete the final project design task.

3 Design and Implementation of Project-Based Teaching

The essence of the project driven teaching method is to take the project as the leading role, so that students can learn spontaneously and actively by implementing a complete project. Students can truly understand how to apply theoretical knowledge in practice during the implementation process of the project. This teaching mode emphasizes the development of students' autonomous learning ability, practical ability and comprehensive application ability. For this course, students' goal is to complete the design of a comprehensive energy system security protection scheme. The teacher releases the course project tasks at the beginning of the semester. Modular teaching is used during the teaching process. When students finish learning a module, they also need to complete the design task of this module. At the end of the semester, students will complete the whole design of security scheme after completing all modules. The project-based teaching method helps students to have a certain engineering practice ability on the basis of having theoretical knowledge. The design of overall teaching plan is shown in Fig. 1.

3.1 Theory Teaching

The main task of theory teaching is to enable students to understand and master the basic theoretical knowledge of cyber security technology. As a core professional course, it requires a high level of theoretical knowledge [7]. In traditional teaching way, teachers normally introduce the basic principles first and then analyze the cases and examples. The theories of this course cover a wide range of areas. It's difficult for students to understand the theories. And they can not understand the corresponding project cases either. This

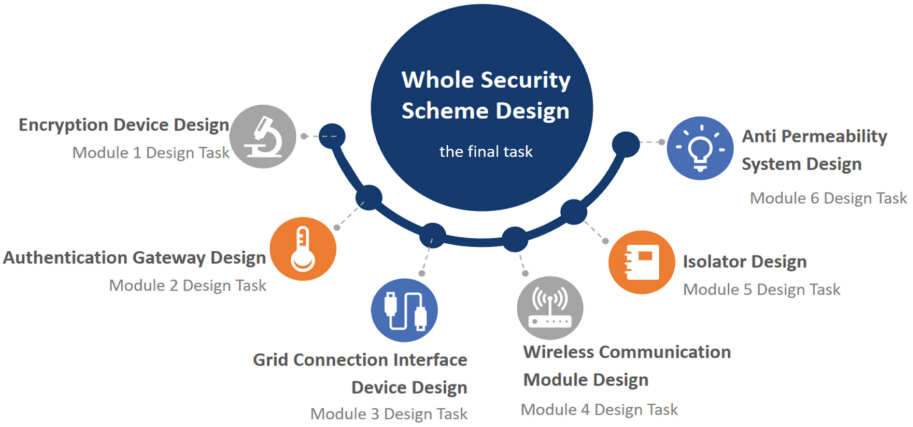

Fig. 1. Design of Overall Teaching Plan

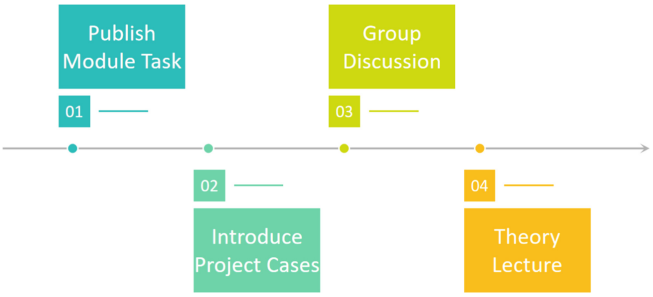

Fig. 2. The Design of Theory Teaching

will causes students to lose learning interests. Under the project-based teaching mode, the teaching concept of project achievement oriented will be adopted. Project tasks will be proposed at the beginning of the semester and completed at the end of the semester, so as to stimulate students' learning autonomy. During a module learning period, the design task of this module will be proposed first, and then the project entity of the module will be introduced, so that students will think before learning the theories. At the beginning, teacher should organize students to discuss and sort out the knowledge points which needed to complete the module design task. Next the teacher explains the theories and takes a lecture. This teaching design can help to make a significant improvement of students' autonomy and learning interests. The concept of problem-based learning case teaching can also be used that students can explore project cases with questions, and then learn corresponding theories, which helps students to deepen their understanding of the basic theory of cyber security course. Figure 2 shows the design of theory teaching.

3.2 Practice Teaching

The are two goals of practice teaching. One is to enable students to understand the application of basic theoretical knowledge in engineering cases. The other is to improve

students' practical ability that they can apply theory to practice and solve new engineering problems [8]. In this course, the practice class hours account for half of the total class hours. That means both theory and practice are important for cyber security learning. Therefore, students need to deepen their knowledge understanding through practice immediately after learning basic theories. In the design of practice teaching, basic experiments are arranged to students for each knowledge point, which are mainly confirmatory experiments. On the one hand, it helps students consolidate and deepen basic theories. On the other hand, it prepares for the subsequent completion of module design tasks and overall project scheme design tasks. During the period of each module learning, when the students complete all the basic experiments of the module, they will do the module design task immediately. After the completion of all modules learning, students will begin to design a complete security project. With such teaching design, students complete the process that know about real project first, then learn about theories, and finally back to design project.

3.3 OBE-Based Grade Evaluation

The view of outcome-based education (OBE) was first put forward in 1981. It requires teachers to clear what results should be achieved after students' learning experience [9]. The teaching objective of this course is to enable students, after learning this course, to have a solid theoretical knowledge of cyber security, engineering practice ability and comprehensive application ability. It requires students to understand the importance of cyber security technology in different fields and make great efforts to become a professional in the field of cyberspace security [10, 11]. Therefore, diversified assessment methods should be designed. It can evaluate students' abilities from different dimensions as theoretical ability, engineering practice ability and comprehensive application ability. This evaluation system can cooperate with project-based teaching and follow OBE concept. The completion of assignments is used to evaluate theoretical ability of students. The online discussion evaluates student the ability of self organized learning. During the each period of module learning, the completion of the basic experiments and the phased design tasks will be taken as the assessment of the practical achievements to examine the students' practice ability. At the end of the semester, students will be required to accomplish the whole design of security protection project as their final examination in order to evaluate the students' comprehensive application ability. So in this grade evaluation system, the score arrangement is shown as Fig. 3, including assignments 10%, online discussion 10%, practice (basic experiment + module task) 30%, and the final task (whole project scheme design) 50%.

4 Application of Digital Experimental Platform

The reason we use project-based teaching mode is that we hope students get to know about the project functions in real industry. During their learning process, they can improve both theoretical and practice abilities at the same time. So during our teaching, we use two digital platforms to satisfy students' learning. One is an experimental platform. The other is a virtual simulation system.

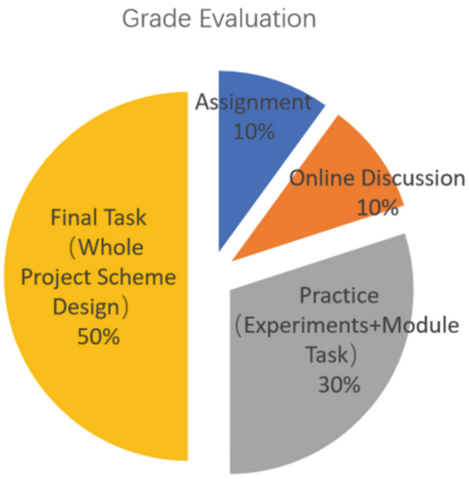

Fig. 3. Score arrangement of Grade Evaluation

4.1 Experimental Platform

In this platform there are different themes of experiments resouces about cyber security. There are two main functions in this platform which are very helpful for our teaching: theories reviewing and basic experiments. So this platform is very suitable for students after they finish theoretical learning. They can review knowledge first, then do basic experiments. Most experiments are elementary experiments for verifying the principles.

Here gives an example of basic experiments on this platform. After learning about Dynamic Host Configuration Protocol (DHCP), students can use this platform to do **the experiment of DHCP Attack and Defense**. There exits a real situation in this experiment. A DHCP attack occurred in the network of an enterprise. Someone set up a fake DHCP server (rogue DHCP server) without permission, causing the client PC to fail to obtain the correct IP address information, so that employees cannot access network resources. The network administrator should use the DHCP monitoring function to improve the network security.

The network topology is shown in Fig. 4. In this experiment, students should follow this topology to build the enterprise network in the platform. First They should finish the configuration of DHCP server, rogue DHCP server, core switch SW1 and access switch SW2. Then students should consider how to use DHCP monitoring in this network. Moreover, they should observe the result before and after monitoring.

In this experiment, students can use following commands to realize DHCP monitoring:

SW1(config)#ip dhcp snooping.

SW1(config)#interface fastEthernet 0/1.

SW1(config-if)#ip dhcp snooping trust.

Most students can get the results of these two situations. Without DHCP monitoring, it can be observed that the client PC gets wrong IP address from rogue DHCP server. By using Ethereal to capture the message on the client PC, it can be observed that the client

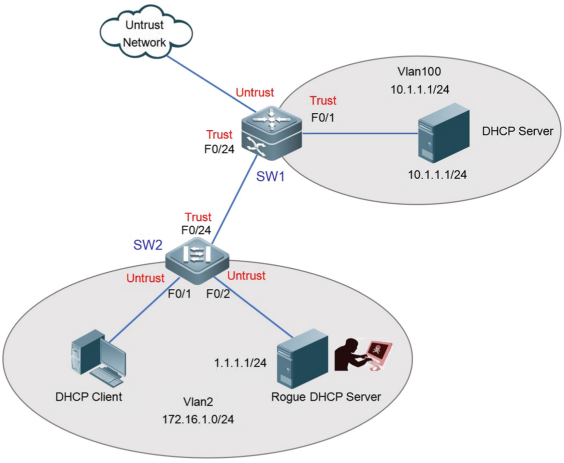

Fig. 4. The network Topology of Experiment

Table 2. Result of dhcp attack and defense experiment

Situation	The client PC gets IP address	The DHCP offer message captured by Ethereal
Without DHCP monitoring	Physical Address. . . . . : 00-15-F2-DC-96-A4 Dhcp Enabled. . . . . : Yes Autoconfiguration Enabled . . . . : Yes IP Address. . . . . : 1.1.1.2 Subnet Mask . . . . . : 255.255.255.0 Default Gateway . . . . . : DHCP Server . . . . . : 1.1.1.1 DNS Servers . . . . . : 202.106.46.151 202.106.0.20	No. Time Source Destination Protocol Info 1 0.000000 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0xe516f721 2 0.000858 1.1.1.1 1.1.1.2 ICMP Echo (ping) request 3 0.002351 10.1.1.1 172.16.1.2 ICMP Echo (ping) request 4 0.502732 1.1.1.1 1.1.1.2 ICMP Echo (ping) request 5 0.502822 10.1.1.1 172.16.1.2 ICMP Echo (ping) request 6 1.002743 1.1.1.1 255.255.255.255 DHCP DHCP Offer - Transaction ID 0xe516f721 7 1.003091 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0xe516f721 8 1.003894 1.1.1.1 255.255.255.255 DHCP DHCP ACK - Transaction ID 0xe516f721 9 1.004165 172.16.1.1 172.16.1.2 DHCP DHCP Offer - Transaction ID 0xe516f721 10 1.009812 AsustekC_dc:96:a4 Broadcast ARP Who has 1.1.1.2? Gratuitous ARP 11 1.703923 AsustekC_dc:96:a4 Broadcast ARP Who has 1.1.1.2? Gratuitous ARP 12 2.703887 AsustekC_dc:96:a4 Broadcast ARP Who has 1.1.1.2? Gratuitous ARP
With DHCP monitoring	Physical Address. . . . . : 00-15-F2-DC-96-A4 Dhcp Enabled. . . . . : Yes Autoconfiguration Enabled . . . . : Yes IP Address. . . . . : 172.16.1.2 Subnet Mask . . . . . : 255.255.255.0 Default Gateway . . . . . : 172.16.1.1 DHCP Server . . . . . : 10.1.1.1 DNS Servers . . . . . : 202.106.46.151 202.106.0.20	No. Time Source Destination Protocol Info 1 0.000000 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0xb76955a9 2 0.003803 ZyElandt_71:a5:4f Broadcast ARP who has 172.16.1.2? Tell 172.16.1.1 3 1.001166 172.16.1.1 172.16.1.2 DHCP DHCP Offer - Transaction ID 0xb76955a9 4 1.005541 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0xb76955a9 5 1.009046 172.16.1.1 172.16.1.2 DHCP DHCP ACK - Transaction ID 0xb76955a9 6 1.011269 AsustekC_dc:96:a4 Broadcast ARP who has 172.16.1.2? Gratuitous ARP 7 1.011914 10.1.1.1 172.16.1.2 ICMP Echo (ping) request 8 1.078342 AsustekC_dc:96:a4 Broadcast ARP who has 172.16.1.2? Gratuitous ARP 9 2.078308 AsustekC_dc:96:a4 Broadcast ARP who has 172.16.1.2? Gratuitous ARP

has received the DHCP offer message sent by the rogue DHCP server. According to the DHCP protocol, the client will use this message. After configuring DHCP monitoring, it can be observed that the client PC gets correct IP address. Because the monitoring function is configured, the switch discards the response message sent by rogue DHCP server. When the client captures the message through Ethereal, it can be observed that the client does not receive the message sent by rogue DHCP server.The results of two situations are shown in Table 2.

4.2 Virtual Simulation Platform

This platform can simulate industrial engineering project running. It also can provide different virtual industrial situations. It is more suitable to help students do some extended experiments and tests. Students can do their own design of project and do some tests to

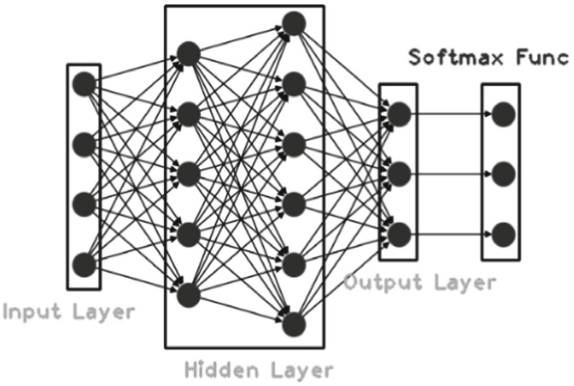

Fig. 5. Deep neural network (DNN) model

Table 3. Test result of design scheme

Column	Average score of network situation
Actual situation value	84.56
Original model	78.92
Designed model	81.85

verify their ideas. Most of them choose to complete their module task and final design on this platform.

Here shows an excellent design scheme from student. This student also used this design scheme to apply for a university level student research project. This design is mainly for implement a cyber security situation assessment model, which can help network administrators predict network security trends. In this design, Deep neural network (DNN) was used to build the model (shown as Fig. 5). Then the student applied appropriate algorithms to finish the model training. He also did some test to verify his design and algorithms. The test result is shown in Table 3. The experimental result shows that his design is effective.

5 Conclusions

Cyber security technology is developing fast Nowadays. The demand for professionals of cyber security is also growing. So this research focuses on how to training excellent cyber security professionals. The author proposes using project-based teaching mode in cyber security course. It is so important to develop students learning ways that they can get familiar with theories and knowledge and complete the application of theories in real industry. One of the advantage of Project-based teaching mode is that it can help students study autonomously. During the project learning process, students explore the project, and they will find solutions actively when they meet problems. This mechanism can help students make a good habit of study.

In this paper, the author mentioned how to combine real engineering project with course and how to match the chapters with the components of the project. It was also described how to use engineering project to introduce the knowledge of theories, and how to organize practice training. In the research, the grade evaluation system was also be built, which evaluated students' different kinds of abilities. In order to better implement project-based teaching, digital platforms are also utilized for practice training. Students can use both two platforms to do elementary experiments and do their project design task. All these ways can help students get familiar with cyber security knowledge and make use of it.

For further research, school-enterprise coorperation will be considered in the cyber security professionals training. On the one side, experienced engineers can be employed as faculties. They will bring plenty of real project cases to the classroom, which can help students know more about cyber security. On the other side, students can do their curricular practical training in enterprise. Enterprise can also provide some internship positions for students. In this way, it can help students know the application of cyber security in real industry.

Acknowledgment. The research is sponsored by "2022 Teaching Reform Project of Guizhou University of Commerce (Project No. 2022XJJG09)".

And "Guizhou Provincial Department of Education Youth Science and Technology Talent Growth Project, China (Project No. KY [2021]271)".

And "Science and Technology Planning Project of Guizhou Province, Department of Science and Technology of Guizhou province, China (Project No. [2020]1Y282)".

References

1. C. V. Gonzalez and G. Jung, "Teaching Cyber Security Topics Effectively in a College or University with Limited Resources," 2019 Int. Conf. Comput. Sci. Comput. Intell. (CSCI), 2019, pp. 832–836.
2. J. Mao, J.W. Liu, T. Shang, Z.Y. Guan, Z. Zhang, T.G. Xu, "Exploration and Practice of OBE based Closed Loop Classroom Teaching Method for Network Security Course," Ind. Inf. Educ., no. 04, pp. 42-47, 2019.
3. Z.Q. Wang, Z. Wang, Z.Y Wang, "Exploration of teaching mode of network security courses based on flipped classroom," J. Beijing. Inst. Electron. Sci. Tech., no.04, pp. 103-109, 2021.
4. L. J. Thomas, M. Balders, Z. Countney, C. Zhong, J. Yao and C. Xu, "Cybersecurity Education: From Beginners to Advanced Players in Cybersecurity Competitions," 2019 IEEE Int. Conf. Intell. Secur. Inf. (ISI), 2019, pp. 149-151.
5. J.J. Feng, "Research on the main problems and countermeasures of Flipped Classroom in college teaching practice," 2020 Int. Conf. Comp. Eng. Appl. (ICCEA), 2020, pp. 166–169.
6. R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa, "Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications," IEEE Access, vol. 8, pp. 151019-151064, 2020.
7. M. D. Workman, J. A. Luévanos and B. Mai, "A Study of Cybersecurity Education Using a Present-Test-Practice-Assess Model," IEEE Trans. Educ., vol. 65, no. 1, pp. 40-45, Feb. 2022.

8. K. Yonemura et al., “Cybersecurity Teaching Expert Development Project by KOSEN Security Educational Community,” 2021 IEEE Global Eng. Educ. Conf. (EDUCON), 2021, pp. 468–477.
9. W. G. Spady, Outcome-Based Education: Critical Issues and Answers. Arlington: American Association of School Administrators, 1994.
10. A. T. Sherman et al., “Project-Based Learning Inspires Cybersecurity Students: A Scholarship-for-Service Research Study," in IEEE Secur. Privacy, vol. 17, no. 3, pp. 82–88, May-June 2019.
11. R. Velea, V. Ilie and I. Bica, “Applying Parallel and Distributed Computing Curriculum to Cyber Security Courses,” 2020 IEEE/ACM Workshop Educ. High-Perform. Comput. (EduHPC), 2020, pp. 12-18.