Experiences from a Time-Condensed Computer Security Class

Weiqing Sun
Dept. of Engineering Technology
University of Toledo
Toledo, Ohio, USA
wsun@eng.utoledo.edu

Abstract—**In this paper, the author shares the experience of teaching a time-condensed version of an undergraduate level computer security class in six-week's time. In this way, it can meet the diverse scheduling requirements and ensure that students be educated at a faster pace to cope with the escalating cyber security threats. In order to effectively run the class, the instructor incorporated a combination of instructional approaches into different course components, including comprehensive traditional lectures, hands-on lab assignments and final research projects. Each of the course components was carefully customized and designed to fit into the condensed course schedule without sacrificing the effectiveness. Although it was a busy class on a tight schedule, both the instructor and the students enjoyed this condensed version.**

Keywords-Condensed course design; information security; security education; virtualized networks; undergraduate research

I. INTRUDUCTION

As worldwide security threats keep escalating at a rapid pace, education in computer security becomes more important and more urgent. It is high time to impart basic computer security knowledge to general Internet users, not only on a larger scale, but also at a faster pace. Cyber security education at universities and colleges has played a central role in the process, but it should also adapt and meet the new challenges. Previous work [1, 2, 8] has identified the challenges, directions and approaches for security education. [3] shares the successful experience of teaching computer security in a small college. But to the best of the author's knowledge, little work has been done to design and provide time-condensed versions of computer security courses to better cope with the above-mentioned challenges. By providing the time-condensed version, we can train students at a faster pace and have more flexibility in scheduling the security courses.

At The University of Toledo, the computer science and engineering technology program focuses on undergraduate education. What makes it unique from other traditional computer science programs is that hands-on skills are emphasized across the complete curricula of the program. This computer security course was recently added to the curricula for students with senior standing, as a result of the increasing demand of computer security education. Although it is relatively new, the course has been drawing more and more attention from both the students and the department. The objective of the course is to provide students with a comprehensive knowledge of computer security and to train students with practical hands-on skills in protecting computer systems from malicious attacks. In the summer of 2009, the security course was scheduled as a 6-week class in the second summer session to accommodate requests from the students who have full-time duties in the first summer session. Compared with the traditional course which runs in 16 weeks during regular spring or fall semesters, this course is much more time-condensed. As a result, the course would require four prolonged meetings (two and a half hours) each week and all the activities involved in the course would conclude in exactly six weeks. This arrangement poses a big challenge for the course planning:

1. The load of the time-condensed course should be comparable with that in regular semesters.
2. Due to the faster pace, the intensity of the course will be significantly higher. Students will have less turn-around time to study and digest the course materials. And the instructor will have less preparation time between different topics.
3. The course materials cannot be simply condensed to fit into the time-condensed version. For instance, projects that take a relatively long time to finish will become infeasible to deploy. It calls for creative methods to prepare course materials.

Despite all of these challenges, the offering of this time-condensed course should not lower the requirements so as to prevent it from achieving the original course objective.

II. PLANNING

In an effort to address all of the above-mentioned problems and effectively run the fast-paced security course, the instructor adopted a combination of different instructional approaches to achieve the goals for this course:

1. Traditional lectures: to get students familiar with basic knowledge in the broad areas of computer security;
2. Hands-on lab assignments: to train students on how to apply the theories learned from lectures to solve real-world security problems;
3. Final research projects and presentations: to give students an early experience of performing research in computer security area and an opportunity to present their work to the audience in a conference-like setting.

The three course components covered different aspects of computer security – theory, practice and research

respectively; and they were especially designed and sequenced to fit into the course schedule. In the six-week instructional period for this course, the class met four times each week. For each of the class meetings, the instructor made use of the first 1 to 1.5 hours for the traditional lectures, and then allocated the subsequent 1 to 1.5 hours for hands-on lab sessions. From the third week on, the instructor started to use part of the lab sessions to discuss the final projects. And the final project presentations are scheduled to be on the last two days of the class.

In the rest of the paper, the author describes the three customized course elements covering the above approaches in Sections III, IV and V, ethics education are discussed in Section VI, course evaluations from both students and the instructor are provided in Section VII, finally the conclusion appears in Section VIII.

III. LECTURES

In our computer science program, this is currently the only course that focuses on computer security. Its primary objective is to provide students with a comprehensive knowledge of computer security. To achieve this, the instructor adopted the traditional lectures approach to convey the basics in computer security. Special considerations were used when deciding the lecture materials for this condensed course. On the one hand, the lecture contents should be very broad so as to provide a good coverage of basics in computer security. On the other hand, the contents of the lectures should not be too difficult because most students would not have any background in computer security. This required a balance when deciding upon the coverage and difficulty of lecture contents. Based on this reasoning, the instructor customized the lectures in the way that they cover a large portion of computer security fundamentals, including basic cryptography, security policies, network security, program security and systems security. In the meantime, the lectures would not provide in-depth discussions in any particular area. The schedule of the lectures fitted the condensed course very well and it is summarized in Table I. For example, as demonstrated in Table I, in the second week, the instructor spent two lectures discussing basic cryptography, and one lecture was devoted on key management and authentication, respectively.

TABLE I. LECTURE SCHEDULE

Week	Lectures
1	Access control and security policies.(2) Confidentiality policies.(1) Integrity policies.(1)
2	Basic Cryptography.(2) Key Management.(1) Authentication.(1)
3	Confinement problem.(1) Auditing.(1) Malicious logic.(2)
4	Intrusion Detection.(2) Network Security.(2)
5	Systems Security.(2) Programs Security.(2)
6	Research Topics.(2) Student Presentation.(2)

Unlike a traditional 16-week class, students in this condensed class would have less time to study between lectures. And they could easily get overwhelmed with the amount of course materials delivered in a short period of time. Therefore a quick feedback mechanism was deployed to help mitigate this problem. In particular, the instructor employed weekly quizzes in order to evaluate promptly how well students understood the lecture materials. The questions in the quizzes were used to examine the important concepts (e.g., "What are the typical security threats?") as well as to check how well students learn to apply the basic concepts in practice (e.g., "What configurations have you made to your computer system in order to enhance its security?"). And based on the feedback collected from the quizzes, the instructor would make corresponding adjustments to the lecture contents and the delivery method, for example, the instructor would regularly provide concise summaries of the topic before starting a new one after observing that some of the students lost track of the important points and did not do a satisfactory job in the quizzes.

In summary, customized lectures and weekly quizzes were the components deployed in this class to cover the basic concepts in computer security.

IV. LAB AND LAB ASSIGNMENTS

The second important component of this condensed course is hands-on lab assignments. The lab assignments played an important role in enhancing the practical skills for students in this class.

A. Lab Platform

Previous studies on hands-on labs [4, 5, 6] have demonstrated the effectiveness of teaching computer security using dedicated lab environments. Although this course was a condensed version, the instructor incorporated the hands-on lab component to enhance the student learning experience. Due to the fast pace of this course, the instructor needed to choose a lab environment that is friendly to both users and administrators. In the meantime, frequent advising would be given to students for prompt adaption to the lab environment.

In support of the lab assignments, the instructor made use of V-NetLab [4], because it fits the course requirements very well. V-NetLab is a platform that can provide identical isolated virtual networks based on user specifications. It is lightweight, cost-efficient and user-friendly. We configured V-NetLab platform on a small physical LAN consisting of a Dell PowerEdge 2950 Server and a Dell Optiplex Desktop computer. The Dell Desktop was configured to be the gateway to the virtual lab environment, and the server was configured to host all the virtual networks. This V-NetLab setup is capable of supporting 8 isolated virtual networks with 6 virtual hosts in each network, which is sufficient for the 7 groups of students in our class (each group has two students.) We spent one week's time on installing and configuring V-NetLab on the physical LAN.

In order to access V-NetLab and their virtual networks, students would need to use an ssh client (for example, *putty*) and an XWindows Server (for example, *Xming*) installed on the PC computers in the department laboratory. For students

who also want to have access to their virtual networks at home, they need to install the two pieces of software on their home computers. After that, they can remotely log in to the gateway of V-NetLab, and then run a single start command to show their networks. Upon success, they should have a few VNC windows displayed, each of which corresponds to one virtual host in the virtual network. Then they can use the pre-configured administrator account to log in to each virtual host and start to work on the lab assignments on their own isolated virtual networks. Once they finish one lab session, they can simply close all the VNC windows, and their virtual networks will resume on the next start command when they come back to their lab assignments.

B. Lab Assignments

The design of a typical lab assignment based on V-NetLab platform involves providing a virtual network definition (the network topology, IP addresses and operating systems for all the hosts in the specified network) and customization of master virtual machine image to include the set of pre-installed software. After the design is done, the instructor will use control commands to pre-create identical isolated virtual networks for each group of students.

The instructor was aware that time-consuming lab assignments would not easily fit into the tight course schedule. Therefore, the following three "condensed" lab assignments were designed, implemented and offered to the students.

Lab1 is a network configuration laboratory, students were asked to find out the static topology of a given network and then configure routing tables to "connect" the network. After that, they were requested to set up a few typical network services based on the specification of the assignment. In this lab assignment, the students need to understand the TCP/IP principles, and know how to use various network management tools such as *ifconfig* and *route* to configure the network specifics. Moreover, they need to learn how to configure typical network services such as ssh, www and nfs. In essence, the knowledge that students gained from this lab builds a good foundation for subsequent lectures and lab assignments. Students were given one-week's time to finish up the first lab assignment.

Lab2 is a network discovery game, it consisted of two phases, and each group would play two different roles in the two phases of the game. In the first phase, each group would act as "*the hider*". They would configure their networks in the manner that they would like to, including setting up different services on different hosts, and writing scripts/programs to incur constant dynamic traffic to access the services (*cronjob* was used to generate the dynamic traffic constantly). By the end of the first phase, each group needed to document the characteristics of their networks. In the second phase, students changed the role into "*the seeker*". Each group would be randomly assigned to discover a network prepared by another group. As a matter of fact, only the instructor knew whose network was currently being discovered by which group. Moreover, in this phase, instead of being granted accesses to all the hosts in the network so as to render it trivial to discover the whole network, only a host

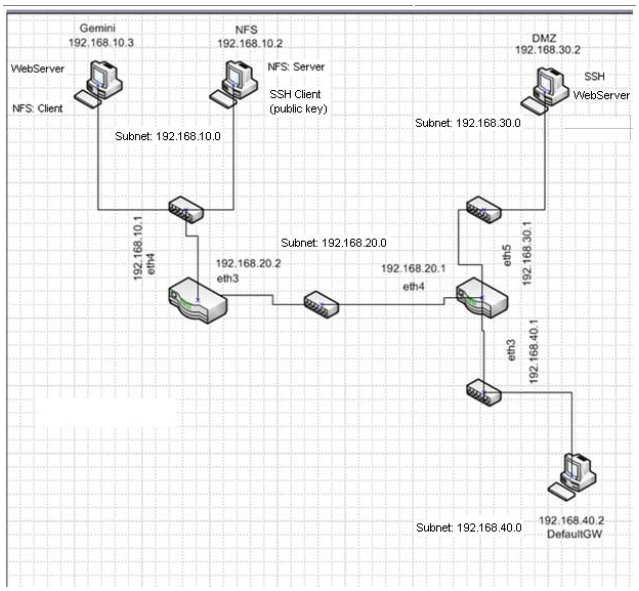

Figure 1. Lab2 network topology (submitted by a student group).

in the network was made open for access. (In the setup, after issuing the start command, only the VNC window for that open host was displayed, while all the other hosts were hidden from the discovering group.) The students would need to use various network discovery tools such as *nmap* and *tcpdump* to learn about the network, including the static layout, as well as the dynamic traffic characteristics. Once they finish this lab assignment, they were requested to write a report to summarize all the findings including the services, service locations, and traffic characteristics, along with the evidence to support their findings. This game took two weeks to finish, with each phase taking one week's time. Fig. 1 is part of the submission from one group in the class, it showed the network topology, and identified the services that were up and running on corresponding virtual host in the network. Right after they turned in their reports for lab2, the students had the opportunity to uncover the mystery—which group had been discovering their own network, and whose network had been discovered by them. Following the pairing information disclosed by the instructor, all the corresponding groups gathered together to check out how much they had discovered from the mysterious network, and then both parties were required to fill up a peer-grading form to provide feedbacks on the performance of their peer groups, including roles for the hiding and the seeking, respectively. The peer-grading forms served as the basis for the grading of the second lab.

Lab3 is a laboratory on firewall configuration. In the lab, students were provided with a network that is a miniature of the typical enterprise network, with standard network services installed and configured in advance. In the network, there were two firewalls — internal and external firewall. Students need to configure *iptables* rules on the two firewalls to secure different portions (in particular, the internal network and the DMZ) of their network. Due to the time constraints, most groups could not completely finish this lab

assignment, as they have to put most of their efforts on the final projects and presentations. Therefore, the instructor made it an optional lab and give extra credit for those who submitted their lab reports.

Overall, the three lab assignments provided a good coverage for the security practices on a typical network environment. Most students were able to enhance their practical skills by working on these lab assignments.

V. FINAL PROJECTS

The purpose of the final project is to familiarize students with research in topics in computer security. As demonstrated in [7], it is valuable to incorporate research in undergraduate level computer security courses. Normally, in a 16-week computer security course, students would be asked to design and implement a complete solution to a given problem. However, this would not fit into the tight schedule governing this fast-paced class. Hence, the instructor adopted a survey-report-presentation style in performing the final project. To help students choose an appropriate project, the instructor created a candidate project pool, which included special topics that were not covered or not discussed in details in the lectures. Students could also propose projects of their own interests, as long as the proposed projects are approved by the instructor. The final projects began in the third week, when each student decided upon a research topic that he or she was interested in. After that, each spent three weeks in surveying the state-of-art techniques and then summarized his or her finding along with his own insight into a written report of 6-8 pages. When working on the final projects, students would discuss the progress with the instructor every few days to make sure it was on the right track. The instructor would then give suggestions for the research methodology and provide pointers for references whenever necessary. The selected research topics spanned a broad area of computer security, including wifi security, spyware, flashworm, hardware security, study of worm *Conficker*, study of an attack (for example, buffer overflow, SQL injection and DoS attacks), digital forensics, study of Kerberos and practical security practice in a commercial organization.

There are two major tasks in the final project: the final project report and the final presentation. In addition to writing the final reports, each student was required to give a 20-minute presentation in front of the whole class. In the 20-minute allotted time, 18 minutes were devoted for the presentation; 2 minutes were reserved for questions and answers. The whole format closely followed the standard conference style, and it was open to the public.

In order to help students to do a satisfactory job in their reports, the instructor collected a few informational online resources for them to refer to. Moreover, the instructor worked closely with the students by providing constant feedbacks on improving their reports and the presentation slides. In order for them to have a good feeling about a research presentation, the instructor gave a demonstration research talk on his own research project right before the students' presentations. It achieved the desired results as expected. Overall, students did an impressive job during the final presentations. One student who worked on wifi security shared his experience of "attacking" a wireless router at home and recommended practical protection measures. Another student who has been working in a company for years presented the security practices in his organization and enforced the concept that "security is a continuous process". These two are among the many presentations that were both informational and entertaining.

The final project—in place of the final exam—represents 30% of the total grade. The report and presentation are of equal weight in the grading. The instructor judges the final report based on the content and writing. The final presentation is judged based on the content and format of the slides, presentation of the materials, and the comprehension of the related materials.

VI. ETHICS

The instructor clearly understands that ethics is an important part of computer science education, especially in the context of computer security. Throughout the course, professional ethics were instilled in every course element whenever possible. In the lectures, the instructor gave examples of computer hackers, and encouraged the whole class to discuss upon the topic, to form an ethical view of computer attackers. In the hands-on lab sessions, the instructor emphasized the lab policy that students should never use skills learned from the class to perform any illegal operations that would disturb the public networks. In the final projects, one student gave a nice presentation that covered important laws and regulations regarding computer security. All of these helped students to be ethical as well as skilled in the area of computer security.

VII. EVALUATIONS

Since this is the first trial for a time-condensed computer security class, evaluations play an important role in identifying the current problems and helping to improve the quality of the class in the future.

A. Student Evaluations

In order to evaluate the effectiveness of the course, the instructor designed an after-class evaluation form. It contained the following questions regarding this course:

1. "How do you rate your knowledge level of computer security after this course?"
2. "How do you rate this course in general?"
3. "How do you think of the final project and final presentation?"
4. "What are your suggestions for improving the course?"
5. "Will you be interested in taking advanced security courses in the future?"

Students were requested to fill in the forms anonymously on the last day of the class.

Regarding to Question 1, most of the students rated 6~9 out of 10, which is a considerable improvement compared with scores 1~5 based on the before-class survey. That was a reasonable indication that the objective of this course had been fulfilled. For Question 2, all the students rated this course as good, as one student wrote "I enjoyed this class a

lot and learned a great deal." It showed that students were not adversely affected by the condensed format. For Question 3, although some of them expressed concerns on the final presentations because of lack of previous experiences, most of the students were in favor of this configuration. Some of them felt excited about the final project and presentation—

"Good exposure to topic of interest to presenter, broad exposure to various topics for rest of class."

"Love it. Thought it was a great idea! Liked it because, you get to learn about other topics of interest. Also gain confidence from doing the presentation."

It was expected that some of the students would have difficulty in coping with the final projects and presentations, but the outcome was reasonably good. In Question 4, students provided some constructive suggestions such as having more lab assignments, and developing a more direct relationship between the lectures and the lab assignments. And two of the students expressed their preferences of a regular semester-long course over this condensed version. This was not unexpected because some of students got used to the regular semester-long courses, and had difficulty in catching up with the high-tempo class. For Question 5, most of the students exhibited a strong interest to take the advanced security course if possible. As a matter of fact, the department is in the planning phase to provide more specialized advanced security courses.

Feedback was also collected for evaluating the lab assignments and the V-NetLab platform. Students liked the idea of having V-NetLab to support their lab assignments, which helped them to better understand the concepts in computer security. Overall students rated the virtual lab environment 8 out of 10. The main complaints had been on the performance, because the virtual networks occasionally became overloaded and less responsive due to the limited hardware resources of the current setup. Some of them regretted not having enough time to finish the third lab and even more lab assignments. This could be addressed by rearranging the lab assignments, for instance, by assigning the first lab assignment one week earlier than was offered. They also provided suggestions to further improve the lab environment to make it more user-friendly.

B. Instructor Reflections

When given the schedule of the class, the instructor felt that it was a challenging task to combine the course elements (lectures, lab assignments and final projects) into this time-condensed computer security class. The course planning phase had been a painful process; it was difficult to achieve the course objective with the tight schedule and the available resources. Among all the course elements, the deployment and configuration of V-NetLab platform were the most challenging, considering that it needs to be set up and all the lab assignments need to be implemented in a relatively short period of time.

Upon completion of this course, the instructor is glad to see that this condensed course turned out to be successful as evidenced by the student evaluations, among other feedbacks. The instructor believes that we should never underestimate the students' abilities to adapt to learn. They need challenging tasks to improve themselves at a faster pace.

As a first trial for a time-condensed version of computer security course, it is far from perfect. As pointed out by students, they would like to have more lab assignments than currently offered, and so on. We will take the constructive suggestions from the students to improve this course continuously. The short-term plan is to add more hardware resources to the V-NetLab platform to improve its overall capacity. Then we can support bigger classes because we do expect to have more students to enroll in the course in the future. The next step would be to design additional hands-on lab projects that can establish a more direct relationship with the lectures.

VIII. CONCLUSIONS

This paper presented a time-condensed version of an undergraduate computer security course. It adopted a combination of instructional approaches and incorporated them into the customized course components, including traditional lectures, hands-on lab assignments and final projects. The student evaluation demonstrated the effectiveness of this course. Although the condensed version of a computer security course was proposed as a result of a special scheduling arrangement, we believe that it can enrich the experiences in computer security education. The deployment of the condensed class can enable people to learn basic knowledge in computer security at a faster pace to encounter the fast-evolving security threats. For universities that offer short-semester courses, it can serve as a good reference. It can also be used as a comprehensive training program for industry partners that need to train their employees with basic security knowledge.

ACKNOWLEDGMENT

Our special thanks to R. Sekar at Stony Brook University for providing the V-NetLab software, Linda Beall and anonymous reviewers for the constructive suggestions for improving the paper, Arun Ponniah Sethuramalingam and Ganesh Sangle for giving instructions on the deployment of V-NetLab, Jason Mayer and Chris Koehnke for helping to set up V-Netlab platform at the University of Toledo.

REFERENCES

[1] M. Bishop, "The State of INFOSEC Education in Academia: Present and Future Directions", Information Systems Security Education Colloquium, Maryland, April 23-24, 1997, pp. 19-33.

[2] C.E. Irvine, "Challenges in Computer Security Education", IEEE Software, Sept./Oct. 1997, pp. 110-111.

[3] C. LeBlanc and E. Stiller, "Teaching computer security at a small college", Proceedings of the 35th SIGCSE technical symposium on Computer science education, Norfolk, Virginia, March 03-07, 2004.

[4] K. Krishna, W. Sun, P. Rana, T. Li, and R. Sekar, "V-NetLab: A Cost-Effective Platform to Support Course Projects in Computer Security", Proceedings of the 9th Colloquium for Information Systems Security Education, Georgia Institute of Technology, Atlanta, Georgia, 6--9, June 2005.

[5] J. Hu, D. Cordel and C. Meinel, “A Virtual Laboratory for IT Security Education”, Int. Conference on Information Systems in E-Business and EGovernment (EMISA), Luxembourg, Oct. 2004, pp: 60–71.

[6] J.M.D. Hill, C.A. Carver, Jr., J.W. Humphries and U. W. Pooch, “Using an isolated network laboratory to teach advanced networks and security”, ACM SIGCSE Bulletin, March 2001, v.33 n.1, p.36-40.

[7] D. Schweitzer, J. Boleng, and S. Hadfield, “Providing an Undergraduate Research Experience in a Senior Level Security Course”, Proceedings of the 13th Colloquium for Information Systems Security Education, Seattle, WA, June 1 - 3, 2009.

[8] W. Yurcik, and D. Doss, "Different Approaches in the Teaching of Information Systems Security," Proceedings of the Information Systems Education Conference (ISECON), 2001.