Network Security is one of the core subjects in Bachelor of Information Technology course offered at the Charles Sturt University. The subject covers aspects of information security relating to the wired and wireless networks. The weekly topics provide students detailed knowledge of cryptography, system threats and countermeasures, secure communication, network vulnerabilities and attacks, network defenses, virtual private networks, wireless and sensor networks security, access control and auth ...
Network Security: Contents, delivery and assessments of an undergraduate subject

Tanveer A Zia
School of Computing and Mathematics
Charles Sturt University
NSW, Australia
tzia@csu.edu.au

Abstract—Network Security is one of the core subjects in Bachelor of Information Technology course offered at the Charles Sturt University. The subject covers aspects of information security relating to the wired and wireless networks. The weekly topics provide students detailed knowledge of cryptography, system threats and countermeasures, secure communication, network vulnerabilities and attacks, network defenses, virtual private networks, wireless and sensor networks security, access control and authentication, Internet Protocol (IP) security, vulnerability assessment and security audit, security policy and training. This paper provides the process of subject development, delivery, assessments, teaching critique, and provides results from online subject evaluation survey. The reflection on subject delivery is particularly important to determine if the subject has met its objectives. Results from the subject critique and student evaluation survey are presented and a reflection on how to improve the subject is provided.

Keywords- Network security education, network security subject, network security course, network security teaching and training.

I. INTRODUCTION

Network security has become crucial due to the widespread of Internet and internetworking technologies. Networks are used more often to store the valuable information as compare to fixed storage devices. Network security ensures that valuable information assets are protected while the information move around the wired, mobile ad-hoc and wireless networks. For the Internet and networks to achieve the potential benefits, it is important that all networks are protected from threats and vulnerabilities. Given the importance and sensitivity of most information assets it is vital to design a subject which equips our Information and Communication Technology (ICT) graduates with advance network security knowledge both technically and conceptually. This paper not only presents a network security subject and its delivery but also provides the reflection as result of teaching critique and subject evaluation survey completed at the end of the teaching session.

This subject is one of the core subjects offered in Bachelor of Information Technology course offered by the School of Computing and Mathematics at Charles Sturt University. The author has the privilege to review, compile, coordinate, teach, assess and reflect on the subject which was offered in Session 2, 2009. The unique aspects of this subject are its applied approach. Weekly modules and assessments are designed in such a way that experienced learners can reflect on their real-life network security experience and novice learners can gain valuable knowledge which will be applied when they embark on a network security career.

Students have particularly appreciated the hands-on projects because of interactive nature which provides a real life work experience. Below is the subject description and objectives taken from the Subject Profile:

This subject informs students of aspects of security relating to the operation and management of information technology infrastructure. The subject covers managerial and technical aspects of information security and provides a practical insight into information technology security practices. Upon successful completion of this subject, students should:

- be able to describe various types of threats that exist for computers and networks;
- be able to define the basic terminology associated with computer and information security;
- be able to describe the various physical security components used to protect computers and networks;
- be able to identify methods used to attack information security systems;
- be able to list techniques to enhance information security;
- be able to recognise basic cryptography techniques;
- be able to explain the components and use of a public key infrastructure;
- be able to identify the different types of devices used to secure a network;
- be able to compare and contrast the effectiveness of various firewall architecture;
- be able to define virtual private networks and describe their security aspects;
- be able to describe the security implications of wireless networks;
- be able to outline the role and features of intrusion detection systems;
- be able to apply methods of hardening network infrastructure;
- be able to describe various types of network and computer attacks;
- be able to list security aspects of applications such as email and web services; and
be able to outline aspects of security policies and risk management techniques.

The rest of the paper is organized as follows. Section II presents the subject syllabus which includes rationale behind choosing the textbook, recommended readings and outline the subject content. Subject delivery and teaching is discussed in Section III. Section IV summarizes the assessments. Section V provides the teaching critique and student survey evaluation results. Finally the paper is concluded in Section VI.

II. SYLLABUS

The subject is compiled in close consultation with the industry experts and practitioners in network security. In any subject, having a textbook as a primary source of reference is important. It is very challenging to find all the relevant contents in one book. Especially, books written in Australian context are rare. With careful consideration, Ciampa [1] is used as a textbook in conjunction with several recommended readings [2] – [9]. The subject contents in following section are derived from the prescribed textbook and recommended readings.

Topic 1: Introduction to information security

This topic introduces security fundamentals. It begins by examining the current challenges in computer security and why it is so difficult to achieve. It then describes information security in more detail to see why it is important.

Topic 2: Cryptography

In this topic students learn how the encryption process can be used to protect data. They first learn what cryptography is and how it can be used for protection. Then they examine how to protect data using various encryption algorithms. Students study various substitution and permutations ciphers.

Topic 3: Systems threats and countermeasures

First part of this topic examines the threats and risks that a computer system faces today as well as virtualization and how virtualization environments are increasingly becoming the target of attackers. Second part of the topic provides an overview of the countermeasures to protect the information systems.

Topic 4: Secure communication

This topic addresses network based threats and highlights the importance of firewalls and secure communication. Email is one of the mission critical business applications. However, it is a vulnerable tool. It is very important to ensure the security of communication. This topic describes the need for email security and explores the vulnerabilities associated with e-mails and how to protect against them.

Topic 5: Network vulnerabilities and attacks

This topic gives an overview of network security. Students first examine some of the major weaknesses that are found in network systems. Next, they look at the different categories of attacks. Finally, a study of the different methods of attacks that are commonly unleashed against networks today is conducted.

Topic 6: Network defenses

In this topic, students explore network defenses. They first investigate how to create a secure network through both network design and technologies. Then, they examine how to apply network security tools to resist attackers.

Topic 7: Virtual private networks (VPNs)

This topic explores VPNs as one of the most common types of remote access. Students learn standard VPN techniques and understand the types of VPN systems. In this topic students also learn router security concepts.

Topic 8: Wireless network security

This topic explores wireless network security. Students first investigate the basic IEEE 802.11 security protections. Then, they look at the vulnerabilities associated with these protections. Finally, they examine today’s enhanced WLAN security protections for both personal users as well as for enterprises.

Topic 9: Access control fundamentals and authentication

This topic introduces the principles and practices of access control and authentication. Students first examine access control terminology, the three standard control models, and best practices. They investigate logical access control methods as well. Students then examine the definition of authentication and review how it fits into access control. Next, they look at different authentication credentials and models. Different types of authentication servers and authentication protocols are also explored. Remote authentication and security is also studied in this topic.

Topic 10: IP security

This topic covers AH (Authentication Header) and ESP (Encapsulating Security Payload) which are the main pieces of IPSec (Internet Protocol Security). Students also learn the IP header extensions for carrying cryptographically protected data, and IKE (Internet Key Exchange), which is a protocol for authenticating and establishing a session key.

Topic 11: Vulnerability assessment and security audits

In this topic students begin a study of performing vulnerability assessments, they first define risk and risk management and examine the components of risk management. Students also look at ways in which to identify vulnerabilities so that adequate protections can be made to guard assets. Then they examine audits, the study of audits is broken down into three parts: auditing privileges that users have, auditing how subjects use those privileges, and monitoring tools and methods.

Topic 12: Security policies and training

In this topic students learn how organizations can establish and maintain security. First, they learn about security policies and the different types of policies that are used. Then, they explore how education and training can help provide the tools to users to maintain a secure environment within the organization. Students also study The
Australian ethical, legal and standards frameworks for information security.

III. SUBJECT DELIVERY

The subject is delivered in a session of 14 weeks both face-to-face for on-campus students and via distance education. For on-campus teaching a weekly lecture of one hour and two hours laboratory tutorial is scheduled. CSU Interact and WebEx training sessions are used for distance teaching. CSU Interact is an integrated online learning environment which allows staff and students to access a number of online services as well as several new teaching and learning tools. WebEx is a collection of real-time web conferencing services developed by WebEx Communications Inc., acquired by networking giant Cisco Systems. WebEx Training Centre has become a popular service for online delivery of education/training to distance students.

CSU Interact Modules tool is used to deliver weekly topics. The Modules tool is a lesson builder tool that allows subject coordinators to publish learning sequences that can be created by using a choice of built-in online editing functions. Each topic in a module contained weekly learning objectives, activities, short quizzes, weekly questions and some useful links. The Resources and Forum tools in CSU Interact were frequently used. Lecture slides and other learning material were made available in Resources. Students used Forum to stimulate discussion on their weekly learning. Forum was also helpful to seek help from the fellow students as well as the subject coordinator.

IV. ASSESSMENTS

There are three assessment items with several tasks each in this subject. Assessment-1 which is due in teaching week 5 includes questions on various aspects of the subject studied so far. Assessment-2 is due in teaching week 10 which includes researching advanced topics studied. Assessment-3 is a final examination containing multiple choice and short-answer questions.

A. Assessment 1: Activities

Assessment-1 contains four activities. In activity one student install a keylogger and have the keylogger running while working on activity two which is a decryption exercise. In activity two students are provided with an encrypted quotation and asked to decrypt it. This task requires students to study cryptography thoroughly.

Activity three is an interesting exercise of exchanging encrypted emails. In this activity students are given a public key and asked to send an encrypted email to the tutor. The tutor then uses the corresponding private key to decrypt the message and reply students. Students then verify the digital signature of the tutor. This activity is well liked by the students due to its hands on nature. Finally, students complete a research activity to prepare them for the major assessment task in Assessment 2.

The rationale for this assessment is to enable students demonstrate their understanding of protocols used in network security and encryption methods. In addition the assessment requires students to implement an enhanced level of security within a network application.

This assessment is marked against the following marking criteria:

- Successful installation of the keylogger and providing a log of decryption activity
- Successful exchange of secure emails
- Relevance and accuracy of the research activity.
- Correct use of citations and referencing conforming to APA referencing format.

B. Assessment 2: Research Report and Webliography

In this assessment students are required to write a report of 2000 words on network security and maintain a webliography. The report is to investigate following three aspects:

1. Networks vulnerabilities and defenses
2. Threats to Mobile Ad-hoc Networks (MANETS)
3. Challenges in addressing security threats in Wireless Sensor Networks (WSNS)

Students are expected to research the current literature using references not older than three years. They are encouraged to visit online databases such as ACM Digital Library. APA (American Psychological Association) referencing format is required both in citation and list of references.

This assessment enables students to research several aspects of network security from current literature and present the findings in a report format. Following aspects are the minimum requirements for the report:

1. Introduction
   a. Describe network security
   b. Mention sources of research
   c. Provide a plan of report
2. Network Vulnerabilities and defenses
   a. List known vulnerabilities in networks
   b. Describe the controls available
3. Threats to Mobile Ad-hoc Networks (MANETS)
   a. List wireless weaknesses
   b. Describe controls to counter weaknesses in MANETS
4. Challenges in addressing security threats in Wireless Sensor Networks (WSNS)
   a. Identify security challenges and risks in WSNS
   b. Provide a summary of Key Management in WSNS
5. Conclusion
   a. Summarize the main points of report

In webliography, students are asked to maintain a blog and post at least five blog entries by the due date of assignment. Each blog entry should provide one annotated link related to network security. The blog entries should discuss network threats, vulnerabilities and controls.
C. Assessment 3: Final Examination

The final examination is a closed book examination which covers the entire subject syllabus. The two hours examination consists of 20 multiple choice questions and five short answer questions. Marks are awarded against the accurate expression of ideas and demonstration of understanding of subject objectives, facts and concepts learned.

In order to pass the subject, a student must achieve a mark of 50% in both the overall mark and the final examination (Assessment-3). The percentage value of each assessment item is given in Table I.

<table>
<thead>
<tr>
<th>Assessment tasks</th>
<th>Value</th>
<th>Week Due</th>
<th>Feedback returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment 1</td>
<td>20%</td>
<td>Week 5</td>
<td>Week 8</td>
</tr>
<tr>
<td>Assessment 2</td>
<td>30%</td>
<td>Week 11</td>
<td>Week 14</td>
</tr>
<tr>
<td>Assessment 3</td>
<td>50%</td>
<td>Week 13-14</td>
<td>Not returned</td>
</tr>
</tbody>
</table>

V. TEACHING CRITIQUE

A teaching critique of face-to-face lecture was conducted through a peer review process and subject evaluation by students to comment on the subject teaching, contents and assessments.

A. Peer review

Below are the good practices recognized in the peer review report and recommended enhancements.

Summary of agreed good practices:

- Genuine concerns about the students was demonstrated by asking if they required help with their work especially following up with students who had been absent from class
- Students appeared to be comfortable, this helps create a relaxed learning environment
- Good use of analogy to help with learning
- Clever questioning to quantify if the students really had gained the knowledge
- Good walkthrough of the revision activities at the end of session
- High interest in students’ progress.

Some of the recommended enhancements to teaching:

- Elicit responses to questions by asking questions and waiting for the students to respond before answering.
- Recap the previous lessons
- Embed pictures and graphics in the presentations instead of moving away from the presentation and showing from the websites
- Engage quiet students.

B. Evaluation Feedback and reflection

Students have particularly liked the hands-on exercises of decrypting ciphers and exchange of encrypted emails. With active participation on the discussion Forum and WebEx sessions, students were keen to learn this important area of study. Many students were from the background where they are involved in a profession relating to network security. At the end of the session, an online subject evaluation survey was conducted to collect the students feedback enrolled in the subject in 2009. Overall evaluation mean is 6.11 (out of 7) which is higher than the mean of other subjects taught in the School. The students have responded well to and appreciated the learning activities. Students have particularly liked WebEx sessions, timely feedback on assessments, prompt responses to the Forum postings and emails, up-to-date concepts in the subject, and frequent use of Interact tools such as Blogs, Chat, and Modules.

It is anticipated that in future the subject can gain more popularity and may become a model subject in information security teaching in an undergraduate level course.

VI. CONCLUSION

Education in ICT security has become popular due to digitization in every field of life. The increasing use of online social networks and digital devices which carry enormous amount of sensitive data requires stronger protection of digital information. This paper has presented a subject on network security with a major focus on principles and practices in ICT security. It is anticipated that this subject will become a model subject in information security teaching in an undergraduate level course.

To enhance the teaching in this subject we need to regularly review contents related to developments in vulnerabilities and threats and prepare our graduates to counter those threats. We also need to introduce new hands-on projects, latest hardware and software tools to improve the technical experience, develop active learning activities as well as emphasize the importance of securing information assets.

REFERENCES