A Case Study in Securing Computer Facilities

By
Dr Helen Armstrong
School of Computer & Information Science
Edith Cowan University
Bradford St
Mt Lawley
Western Australia

Phone: +61-8-9370 6856
Fax: +61-8-9370 6100
Email: h.armstrong@ecu.edu.au

Abstract
This paper describes a practical case study used in a unit of study relating to security of computer facilities. The case study has been designed to draw together the theory presented in a number of security units previously completed by the students. The paper discusses the importance of experience in learning and describes the case study content and action requirements. This case study is currently being used within the School of Computer & Information Science within Edith Cowan University for security degrees.

Introduction

The practical nature of both computing and security allow relatively easy application of theory. The use of practical case studies and experiential work in the areas of computer and information security has been illustrated by many authors (see, for example, Baskerville & Straub 1999, Bell et al. 1999, Fillery-James 1999, Irvine 1999, Janczewski & Jonsson 1997, Jendricke & Rannenberg 1999, Lindskog et al. 1999, White & Sward 1999). When combined with reflection and questioning, practical and experiential learning techniques can provide a beneficial learning environment for students. The act of physically putting theory into practice allows students to gain confidence and solidify their comprehension.

Practical application is one of the key elements of deep learning discussed by McKay and Kember (1997). In order to promote deep learning McKay and Kember suggest the following components are necessary —

- A well-structured knowledge base, ie relevant past learning
- An appropriate motivational context resulting in a positive reaction to the learning process leading to a sense of ownership
- Learner activity involving active learning and participating in actual practices, and
- Interaction with others, both vertical Interaction (student-teacher) as well as horizontal interaction (student-student).

In an effort to bring together much of the content of security related units in the computing area, an extended case study has been devised for students enrolled in Computer Science (Computer Security) and Engineering (Security) degree courses at Edith Cowan University. The case study assignment requires students to apply the theory and knowledge from physical security and computer security units. The instructional unit is entitled Computer Facilities Security and is taught in the final year at Bachelor Degree level (third year), and also at postgraduate level. This unit forms part of the degrees of Bachelor of Science (Security), Bachelor of Computer Science (Computer Security) and Master of Science (Computer Security).

The unit focuses on the application of principles and techniques relating to the security of computer facilities and associated environments; including risk assessment, application of problem solving skills, development of security policy and strategies for the protection of computer facilities, design of secure computer networks and physical and logical security relating to computing facilities. The specific topic areas covered are listed in Table 1.

Students are required to have completed pre-requisite units covering areas of computer security, physical security, information security and risk analysis. It is expected that students draw from this previous knowledge in order to complete the case study. The materials for these pre-requisite units are readily available to the students via the Web.

Seminar Topic Areas	**Specific Topics**	**Workshop Topics**
Crime & Security Surveys	Crime & security surveys	Investigation of surveys by CSI/FBI, EW, KPMG, etc.
Physical Security	Physical access security Building and environment security Biometrics	Building security design Biometric identification systems Site visit to observatory Site visit to security company
Logical Access Security	Information classification Login & password control Access control matrices Directories and user views Logical intrusion detection systems	Logical access control systems Intrusion detection systems
EMR & TEMPEST	Electromagnetic Radiation and Tempest	Tempest Exercise
Network Security	Secure network design Network security policy Internet and e-commerce security Communications security	Network design exercise Security policy exercise
Security Management	Security policies and procedures Security responsibility Personnel security Risk analysis Disaster recovery planning	Personnel security exercise DRP strategy exercise

Table 1: Topic Areas covered by the Computer Facilities Security Unit

Details of the Case Study
The organsation studied is a firm in the scientific equipment industry. Their main activity is the supply of a range of technical scientific equipment direct to laboratories, universities and other industrial organisations undertaking scientific testing, processing and research. Equipment supplied varies in size and products are displayed in a ground floor showroom. The organisation sells imported scientific equipment and also manufactures equipment on site. They also provide technical support including repairs, upgrades, etc. for the equipment range sold. In addition, a web site is used to sell equipment. Students are required to analyse the sections within the organization requiring access by the public and design the premises to meet these needs.

The main focus of this organisation is the research activities led by Dr. Jim Wiseman and his assistant Dr. Simone Brane (female). Dr Wiseman s area of specialisation is the study of asteroids travelling through the earth s atmosphere. Preliminary research findings suggest that asteroids not only reflect cosmic light (so they can be seen by an optical telescope), but also emit radio waves (that can be picked up by a radio telescope). Under Dr. Wiseman s guidance, the research team are developing an Astron Synchroniser, to synchronize the activities of optical and radio telescopes as well as store and analyse the data collected.

The company is looking to construct a new three-storey building and students are required to design a secure layout for the building, the computer systems and other equipment. Students are also required to design a secure network architecture and present a disaster recovery strategy for the Research and Development Department. The case study can be seen in Appendix A. Further supporting documentation is published on the web site for student reference.

Administration and Assessment
Incorporated into the unit is two site visits, undertaken early in the semester, and a demonstration of security software tools. The first site visit is the Perth Observatory, where students can see the housing and operations of optical telescopes and the second is a visit to an organization specialising in building security.

The Perth Observatory guided tour takes place during daylight hours unlike most other observatory tours that are conducted at night. The students study the construction of several buildings used to house large telescopes and are shown the different design of domes and operations of telescope control systems.

The second site visit is to a building security company to see electronic alarm and surveillance systems and biometric identification products. This organization also demonstrates to the students the remote control of the systems via mobile phones and the Internet.

A demonstration of security software tools is conducted by the School s technical support team. Software demonstrated includes network mapping tools, network security vulnerability tools and packet sniffers. Students are not encouraged to use these tools on the university networks.

Students are required to submit a written report containing recommendations and their designs. In addition, students must make a presentation to the group describing their solution. The report and presentation carry 60% of the marks for the unit, with the remaining 40% allocated to a final written examination paper. The design report is submitted in two stages, the first stage involves the physical and logical security design, and the second includes network and communications security design, security management and disaster recovery planning requirements. All areas of consideration must be based upon risk, and students must carry out a risk analysis prior to commencing the new design. All solutions must be linked back to the risk analysis.

Teaching Methods

Computer Facilities Security is a unit of study offered both internally and externally. Internal classes comprise a weekly lecture to cover the theoretical aspects and practical workshops in computer laboratories. Although the students must submit an individual assignment, the weekly workshop exercises require group work. Students are encouraged to work on problem areas together and ask questions. The exercises given in the workshops relate in some way to the EE case study, and students investigate given aspects of the topic area for that week.

Unfortunately, external students studying by distance education do not have the opportunity for group work. They are provided with a written external guide book and unit plan. On-line tutorials are offered using chat sessions and the students have a bulletin board for posting messages. The teaching materials used for the course internally are available to all students via the Web, including lecture notes, workshop exercises, and sample materials. In addition, digital photographs taken on the site visits are also available on the Web site.

The approach used was designed to promote greater group interaction and exchange of ideas. The combination of seminars, workshops, site visits and the practical case study assignment allows numerous teaching methods to be undertaken and encourages the building of knowledge based upon theory and experience. This supports Bloom s (Bloom et al. 1956) learning taxonomy, Kolb s (1984) experiential learning model and Mumford s (1991) extended model of action learning.

Students indicated they preferred to interact as a group in discussion and problem-solving in the classroom and laboratories, but wished to submit individual reports for assessment. This would also allow individual creativity in solution design, rather than a solution reflecting a compromise by some or all of the group members.

Student Feedback

The case study was undertaken with a pilot group of three postgraduate students in the second half of 2000. The same case study is currently being run internally for the second time and externally via the Web for the first time. There are currently more than forty students enrolled in the unit.

The feedback from students completing the unit internally in second semester of 2000 has been positive (see Table 1).

Rating Area	Average Rating	% Rating

Organisation	3.44	86
Teaching	3.53	88.25
Assessments	3.50	87.5
Overall	3.49	87.25

Table 1: Unit Evaluation Responses from Students

It appears that the students generally felt that the course was well organised, taught and assessed. Interestingly, the majority of students felt too much material was covered in the unit. Comments from the students on completion of the course generally suggested that the practical nature of the assignment work was the most valuable contribution of the unit to their knowledge and skill base. They also commented that the practical focus of the unit was also enjoyable. The site visits were reported to be extremely helpful and gave the students the opportunity to question specialists in the field.

The unit materials made available via the Web were used extensively by the students. The Web was used as a repository for all the unit material. It provided a useful tool for distributing resources such as lecture notes, workshop exercises, photographs, helpful links to other Web sites, sample examination papers and other teaching materials.

Conclusion

It is felt that practical application of theory in a case study is a beneficial method of solidifying student learning. The group problem-solving activities and development of the building and facility design is part of an intentional action learning approach. Although it is too early to present definitive evaluation of the case study as used in the above context, the early signs indicate some success.

References

Baskerville, R. & Straub, D., (1999) *Internet Groupware Use in a Policy-Oriented Computer Security Course*, Proceedings of WISE 1, IFIP TC11 WG11.8 First World Conference on Information Security Education, June, Kista, Sweden, pp 171-196

Bell, T., Thimberly, H., Fellows, M., Witten, I. & Koblitz, N., (1999) *Explaining cryptosystems to the General Public*, Proceedings of WISE 1, IFIP TC11 WG11.8 First World Conference on Information Security Education, June, Kista, Sweden, pp 221-236

Bloom, B., Engelhart, M., Frost, E., Hill, W. & Krathwohl, D., (1956) *Taxonomy of Educational Objectives: The classification of Educational Goals: Handbook 1, Cognitive Domain,* Longmans, New York

Fillery-James, H., (1999) *Teaching Computer Security — The Art of Practical Application*, Proceedings of WISE 1, IFIP TC11 WG11.8 First World Conference on Information Security Education, June, Kista, Sweden, pp 197-210

Irvine, C.E., (1999) *Amplifying Security Education in the Laboratory*, Proceedings of WISE 1, IFIP TC11 WG11.8 First World Conference on Information Security

Janczewski, L. & Jonsson, E., (1997) *Information Security Experiments in University Environment*, Proceedings of the IFIP TC!! WG11.8 Third Workshop on Information Security Education, May, Copenhagen, Denmark

Jendricke, U. & Rannenberg, K., (1999) A MixDemonstrator for teaching Security in the Virtual University, Proceedings of WISE 1, IFIP TC11 WG11.8 First World Conference on Information Security Education, June, Kista, Sweden, pp 83-98

Kolb, D.A. (1984), *Experiential Learning: Experience as a source of Learning and Development*, Prentice-Hall, Englewood Cliffs, New Jersey

Lindskog, S., Lindqvist, U. & Jonsson, E., (1999) *IT Security Research and Education in Synergy*, Proceedings of WISE 1, IFIP TC11 WG11.8 First World Conference on Information Security Education, June, Kista, Sweden, pp 147-162

Mumford, A. (1991) *Learning in Action*, Personnel Management, Vol. 23 No. 7, July

McKay, J. & Kember, D., (1997) Spoon Feeding Leads to Regurgitation: a better diet can result in more digestible learning outcomes, *Higher Education Research & Development*, Vol. 16 No. 1, pp 55-67

SCITECH (2001) *How Action Learning will Help*, Scitech Curriculum Facilitator s Guide, Retrieved March 7, 2001 from the World Wide Web: http://www.bhtafe.edu.au/scitech/acthtm.htm

White, G.B. & Sward, R.E. (1999) *Developing an Undergraduate Lab for Information Warfare and Computer Security*, Proceedings of WISE 1, IFIP TC11 WG11.8 First World Conference on Information Security Education, June, Kista, Sweden, pp 163-170