A Popular Postgraduate Information Systems Security Course

Kenneth J. Stevens
Rodger Jamieson
School of Information Systems, Management and Technology
The University of New South Wales
Sydney, NSW 2052, Australia
k.stevens@unsw.edu.au r.jamieson@unsw.edu.au

ABSTRACT

This paper describes a popular postgraduate information systems security course and discusses a number of key issues that currently face the course. The course covers a broad range of managerial and technical topics, and makes use of a number of security tools and techniques to complement the theory taught. The paper details the content of the course and outlines how it is taught and assessed. Specific examples of content and methods are provided and, where applicable, insight is offered as to why the course has been arranged in that particular way. The paper also outlines a number of important concerns and issues currently confronting the course. The issues discussed include the coverage of the course, its breadth and depth, the incorporation of new topics and the role of ethics. The paper should be of interest to those engaged in teaching or charged with the development of courses addressing information systems security.

Keywords: Information systems security, education, postgraduate course, syllabus.

1. INTRODUCTION

This paper describes a postgraduate information systems security course and discusses a number of key issues that currently face the course. The course, Information Systems Security, is an advanced elective in a coursework Masters program and its emphasis is the management of information systems security efforts. The course covers a broad range of both managerial and technical topics, and makes use of a number of security tools and techniques.

The first part of this paper describes the course in some detail in terms of its content and the way it was taught and assessed in 2001. Specific examples of content and methods are provided and insight is offered as to why the course has been arranged in a particular way. The second part of the paper outlines a number of important concerns that currently face the course, and discusses the various options explored in regard to these issues.

This paper provides an insight into the "what" and "how" of running a popular IS security course, which should be of interest to those engaged in teaching and development of similar courses.

2. DESCRIPTION OF COURSE

The course described in this paper is "Information Systems Security" (INFS5984), run by the School of Information Systems, Technology and Management, in the Faculty of Commerce and Economics at the University of New South Wales, Sydney, Australia. The course is an advanced elective within the Masters of Commerce program, and represents one standard course of a twelve-course degree program. The course is also available to students undertaking other postgraduate degrees. A parallel undergraduate 'honors year' stream of the course is also offered, but is restricted to students undertaking highly selective degree programs. The course is offered in the first semester (February to June) of each year and has been run since 1991.

2.1 Prerequisites

The course has a number of prerequisites:

1. *Business Data Communications:* An introductory course into networks, interfaces between networks, data communication software and standard communication protocols.
2. *Data Management*: An introductory course into data management principles that addresses simple

and complex file designs, database management systems, approaches to database architectures (hierarchical and relational) and query systems.

3. *Business Information Systems*: An introductory course that addresses the use and management of information systems in business, information systems components and types, and development methods.

The course's pre-requisites are such that postgraduate students must have completed at least one semester of study prior to undertaking IS Security. Undergraduate students can only undertake the course in their fourth year. These restrictions provide some assurance that students have adequate technical background and maturity. The pre-requisites can be waived in light of relevant work experience.

2.2 Participants

The course is a popular option and typically attracts a full complement. One hundred and thirty three students undertook the course in 2001. Table 1 details the programs being undertaken by the participants.

Table 1: Degree Programs Being Undertaken by 2001 Participants

Postgraduate	
Masters of Commerce (Information Systems)	100
Masters of Commerce (other)	2
Masters of Technology Management	6
Masters of Computer Science (various)	7
Other (Diploma, no-award etc)	8
	123
Undergraduate (Honors)	
Bachelor of Commerce (Co-Op)	1
Bachelor of Information Technology	7
Bachelor of Information Systems	2
	10

Overseas students made up approximately two thirds of the participants. These students had little or no employment experience, having commenced postgraduate studies immediately following their undergraduate degree. The others were local students studying on a part-time basis. These students were in full-time employment, typically in information technology. All the undergraduate students had industry experience as their degrees had an industrial placement component. The participants were organized into three classes for seminars and six classes for laboratories.

2.3 Staffing

Two academics staff the course, dividing the teaching, preparation and administration duties between them.

3. COURSE CONTENT

3.1 Emphasis and Orientation

The emphasis of the course is the management of information systems security efforts. The technical side of IS security is not neglected, as a number of technical aspects and security technologies are specifically considered. It does, however, seek to highlight the implications of the underlying technologies, rather than the mechanics of those technologies.

The course is oriented toward the practical application of what is taught and makes much use of real world cases and tools, business settings for assignments, and guest lectures by leading security practitioners.

3.2 Course Objectives

The stated objectives in 2001 were:

"This course aims to review concepts, theory, methodologies and techniques discussed in the IS security literature and current practice. Students will undertake case studies exercises using the University's computing facilities and laboratories to provide them with a better understanding of computerized security techniques used in practice.

Specific learning outcomes from the course will be for students to:

- Understand and apply the concepts and theory underlying IS security;
- Examine and use current methodologies for IS security design and implementation;
- Undertake a review of IS security practice - techniques and methods for securing an organization's information assets;
- Experience current IS security methods by 'hands on' use of current IS security tools and techniques;
- Use the internet to review current research efforts in IS security; and
- Consider and analyze the impact of IS security on organizations and society".

(Jamieson and Stevens, 2001)

3.3 Topics

In 2001, the course schedule was divided into three blocks. Weeks 1 to 4 dealt with the fundamental concepts and provided the framework for subsequent topics. Weeks 5 to 10 dealt with specific security contexts, technologies and practices. Weeks 11 to 14 dealt with the broader implications and ramifications of these practices and discussed emerging trends within the IS security field. Table 2 outlines the topics covered and provides examples of the required readings.

3.4 Reference Material

The reference materials used throughout the course were gleaned from a wide variety of sources including:

- Research papers from IS and IS security journals, such as 'Computer and Security' and

'Journal of Management Information Systems';
- Practitioner articles from professional journals and industry magazines, such as 'CIO' and 'IT Professional';
- Professional body and research center pronouncements and documentation, such as the 'incidents.org' webpage at the Systems Administration Network Security (SANS) Institute;
- Corporate white papers and documentation;
- Government documentation and legislation;
- Industry body technical papers;
- Local and international standards; and
- The mass media.

Table 2: Syllabus for 2001

Week	Topic	Indicative Readings
1	**Introduction** Definitions, history of security, current concerns, IS security participants, and implications of IS security.	
2	**IS Security Management** Introduction to principles of IS security management, roles of IS security personnel, security methods.	Nosworthy (2000) von Solms (2000)
3	**Risk Analysis and Management** Key principles, management's role, standards, introduction Risk Management Software Tool.	Briney (2000) AS/NZS 4360 (1999)
4	**Contingency and Continuity Planning** Key concepts, development of disaster recovery and business continuity plans, risk assessment, business impact assessment, recovery strategies and common pitfalls.	Kelley (2000) Bandyopadhyay & Schkade (2000)
5	**Logical Security and Physical Security** Logical and data security criteria, input controls, database controls, security policies and mechanisms, physical security criteria, access controls, preventive, detective and corrective measures.	Forcht (1994) Zviran & Haga (1999)
6	**Internet Security** Exposures and threats, approaches to attack and penetration (domain name and route analysis), exploitation, case study and demonstration, trends.	Cohen (1999) Hinde (2000)
7	**Cryptography, PKI, Digital Signatures, Gateway Security** Terms, types of attack, protecting against attacks, authentication methods, security policy, technical solutions (firewalls, encryption).	Barber (2000) Richards (1999)
8	**E-Commerce (B2B) Security** Types of e-commerce, SET, PKI, digital certificates, Authentication (NCSA, HTML, user, cookies, SSL, digital certificates, two factor and biometrics), creating security infrastructures for e-commerce.	Wenninger (1999) Van Krugten & Hoogenboom (2000)
9	**Operating Systems Security** Operating system overview, methods of OS security, evaluation of OS security, comparison of UNIX and Microsoft NT.	Microsoft (2000)
10	**Data Base Security** Review of databases, access control, authorization, integrity, security mechanisms	North (1999) Pangalos *et al* (1994)
11	**Legal Issues** Protection of computer assets, copyright, computer abuse, legal aspects of privacy, legal agreements, admissibility of computer evidence in court, laws governing computers, negligence, and management implications.	Dowland *et al* (1999) Newman & Rao (2000)
12	**Ethical Issues** Privacy and surveillance and implications for IS security, IS professional obligations	Shaller (2000) Kravitz & Pugliese (2000)
13	**Student Presentations**	
14	**Emerging Trends: Biometrics** Key concepts, types and uses, procedure and examples, key issues with use (acceptance, acceptability, accuracy, cost and ethics)	Liu & Silverman (2000) Matyas & Stapleton (2000)

In 2001, the course did not use a reference textbook; but instead a selection of papers and other materials from these various sources was prescribed as the reference materials for each topic. Other materials were also used for class activities and assignments. Of particular note were the use of up-to-date web-based news articles in the seminars and laboratories to promote and structure discussions on e-commerce security, cyber-crime and ethics

4. HOW THE COURSE WAS TAUGHT

The teaching philosophy of the course entails students being proactive and responsible for their own learning and staff facilitating this learning. To this end, the course needs to engage the students at different levels and appeal to the participants though a wide range of delivery mechanisms. Student involvement in class is seen as paramount and the course is designed to encourage participation on a weekly basis.

4.1 Delivery

In 2001, the course was delivered via seminars and computer laboratories. A two-hour seminar each week presented various aspects of the topic at hand, worked through case problems, and discussed the more difficult aspects of the topic. The materials used in the seminar, including slides, were made available on the course website prior to the seminar. Guest Lecturers were videoed and the videos were accessible via the course website, using Cisco Systems IP/TV.

A one-hour laboratory session was held each week, in which students undertook activities related to the week's topic. Activities used during the semester included web-based research, group-based casework and discussions, and using software tools.

In addition, outside the class, the students were required to undertake private study, including preparatory reading, structured activities such as answering discussion questions, and group assignment work.

4.2 Industry Involvement

Industry involvement in the course includes guest lectures by industry specialists and visits to businesses' premises. The guest lecturers are seen to provide the students with an insight into real world practice in regard to current security issues. In 2001, practitioners presented:

- *Week 3: Risk Analysis and Management:* Presented by a risk consultant who was involved in the development of Australian Risk Management standard and who developed a software tool used in the course.
- *Week 6: Internet Security*: Presented by consultants from eSecurity Services, Ernst Young Australia.
- *Weeks' 7 Cryptography, PKI, Digital Signatures, Gateway Security and Week 8 E-Commerce (B2B) Security:* Presented by a senior e-commerce security consultant with Dimensions Data.

Site visits involving the entire class have been undertaken in previous years. The visits have involved commercial and government enterprises inviting the students to view their security facilities and meet with their security managers.

4.3 Use of the World Wide Web

The WWW is used as an external information resource for the students (in completion of laboratory exercises and assignments) and by staff (as a source of reference materials). The course website is hosted on the University's WebCT server and provides students with controlled access to course materials, announcements, results, an assignment submission mechanism, discussion forums, and the 'News Watch' page.

In line with the recommendations of McKenzie and Murphy (2000), discussion forum usage is integrated into the course as much as possible and was used extensively during 2001. In Week 11 (Legal Issues), for example, a question was posed for the first laboratory of the week as to whether "denial of service attacks" were illegal in Australia. Students were asked to work in groups and use the WWW to answer the question. Each group's response was posted to the discussion forum. The exercise expanded over the subsequent laboratories with the addition of new questions. As each group could see the responses posted by all other groups along with theirs, a number of tangential discussions grew up. Groups from the earlier labs were also able to follow the discussion that they had initiated. The discussion forums were an effective means of engaging the students in the course.

The 'News Watch' page entailed a list of web-accessible news articles that had recently appeared in the press and related to an aspect of course. Students were the main contributors of articles to the News Watch page.

4.4 Use of Software Tools

In 2001, the students used Audit Risk Language (ARL) to complete their practical assignment. ARL, from Jeff Bergman Pty. Ltd., is an analytical tool for analyzing business risks and control environments. Other tools that have been used in the past offerings of the course include Internet Scanner and Real Secure® Network Sensor from Internet Security Systems (www.iss.net).

The use of some software tools presents problems in terms of the situation in which they are used. Many of the readily available scanning and detection tools are quite powerful in regard to finding and exploiting security weaknesses. Consequently caution needs to be exercised when deciding what software tools to use, especially if the tools will be used on the University network, or any other 'live' system.

4.5 Use of case studies

The practical nature of many of the areas within IS security is such that case studies are the most appropriate means by which participants can gain an understanding of practices and, after analysis, the concepts behind those practices. Case studies are an integral part of the course and are used in all facets of the course. Textbooks, research and practitioner papers, and corporate 'testimonials' are the key sources of cases.

In 2001, case studies formed a major component of student in-class activities in both seminars and laboratories. In Week 4, for example, a video case reporting the disaster recovery processes of an insurance company was used to provide insight into the security implications of disasters and the contingency planning that takes place in regard to IS security.

4.6 Assessment

The assessment of the students is designed to reflect the orientation and emphasis of the teaching. Table 3 outlines the components of the assessment.

Table 3: Assessment Components for 2001

Assessment Component	%*
Participation	10
Minor Assignment (research)	15
Major Assignment (practical)	20
Exam.	55
	100%

* Percentage contribution to overall mark

Participation was assessed on the basis of attendance and involvement in the seminars, laboratories and discussion forums.

The group-based minor assignment required students to investigate 'Info-warfare' and 'Cyber-Terrorism' and write a report in the style of an 'e-journal' article. Each group's html based report was loaded onto the course website.

The major assignment was also group based and required the groups to investigate and analyze the security and contingency planning practices of a business. Activities included onsite visits to the business to interview staff and collect data, the use of ARL to analyze the data and provide reports, and the completion of a report detailing the conclusions and recommendations. The report was presented to the management of the business studied and the class in the form of a presentation.

A project management component in each assignment and a confidential peer assessment at the conclusion of the semester were used to control and moderate group behavior and assist in the allocation of marks to individual group members.

5. CURRENT ISSUES

The rapidly evolving nature of the IS security field is the source of most of the key issues faced by the course. These interrelated issues include the coverage of the course, the breadth and depth of this coverage, the incorporation of new topics, and the role of ethics.

5.1 The Coverage of the Current Course

The ongoing expansion of the IS security field necessitates decisions regarding the substitution of new topic areas for old topic areas. Recent examples of such changes in this course include '*network security and distributed systems security'*, which was 'shunted' across to the Networks and Distributed Systems course so '*Internet Security'* could be added. The emerging area of *'Computer Forensics'* was considered for inclusion in the course, but was ultimately introduced in IS Auditing (a sister course of IS Security). As the opportunity to add additional topics to the course or transfer topics to other course is limited, the question "*what are the key knowledge requirements of an IS security course?"* must ultimately be addressed.

5.2 Determining Key Knowledge Requirements

Most IS security academics would have reasonably firm ideas of what should be considered a core component of any IS security course. As the field continues to expand, there is risk that new areas may be simply added to the core components, creating courses with overly ambitious schedules that strain both students and staff. In determining which areas should be considered 'core' content, a number of key sources have proven worthwhile, including:

- IS security related standards, such as AS/NZS 7799.2.2000, "Information Security Management" (Standards Australia, 2000) and HB 231:2000, "Information Security Risk Management Guidelines" (Standards Australia, 2001)
- Professional organizations, such as The Information Systems Audit Control Association (ISACA) and The Systems Administration, Networking and Security Institute (SANS); and
- The opinions of industry practitioners.

An important issue that arises when determining the key knowledge requirements is depth of the topics covered versus the breadth of the topics covered.

5.3 Breadth versus Depth

The expanding discipline creates difficulties in maintaining the balance between the extent to which a course covers the field and the extent to which it explores each of the topics in depth. There is a temptation to include as much as possible in the course; however, the experience of the staff involved in INFS5984 suggests that new material is typically added

at the expense of the depth of coverage of other material. A strategy that helps overcome this problem is to apply the fundamental principles to just one key technology. E-commerce is currently the key technology that is covered in depth (in Weeks 6, 7 and 8, and in the assignments). When addressing the issue of balance between depth and breadth, the issue of which new areas should be incorporated into the course arises.

5.4 New Topics

Covering emerging trends and technologies provides student with an awareness of what they can expect in the future. It is, however, simply impossible to cover every new trend in depth. The strategy used in INFS5984 is to provide a general overview of emerging trends and technologies and then focus on one in detail. In 2001 that area was biometrics. The professional literature is used as the key source of information regarding emerging trends. The emerging trend of ethics in IS security seems, however, to require a different treatment.

5.5 Role of Ethics

As the role of IS security in society gains attention, it would seem important that the IS security managers of the future examine the role of ethics in IS security in some depth. As a formal part of the curriculum, ethics often appears remote from the student's experience. To overcome this problem, the use of contemporary examples, such as hacking and piracy, appeared to successfully stimulate debate about the nature and role of ethics and ethical behavior. These concepts can be extended to the students themselves in the personal responsibility they need to accept in the use of security tools and the confidentiality observed when carrying out assignments. The professional codes of conduct of the relevant professional bodies provide direction and material in this regard.

5.6 Conclusion

A number of ongoing issues face those involved in design and delivery of information systems security courses. These issues are driven, for the most part, by the rapid evolution of the field and revolve around what should be in an IS security course, and how they should be determined. A number of key recommendations can be drawn from the experience of the academics in this course. Firstly, focusing in depth on a particular context can assist in getting the right balance between the breadth of coverage and the depth of coverage of material and secondly, ethics is a vital area and needs to be made relevant and accessible to the students.

6. REFERENCES

Bandyopadhyay, K. and L. Schkade [2000], "Disaster Recovery Planning by HMOs: Theoretical Insights." Health Care Management Review 25(2), pp. 74-84.

Barber, R. [2000], "Implementing Public Key Infrastructures in a Dynamic Business Environment." Computer & Security 19(3), pp. 230-233.

Briney, A. [2000], "Security Focused - The 2000 Information Security Industry Survey." Information Security Magazine, September, pp. 40-68.

Cohen, F. [1999], "Simulating Cyber Attacks, Defences and Consequences." Computers & Security, 18(6), pp. 479-518.

Dowland, P.S., S.M. Furnell, H.M. Illingworth and P.L. Reynold [1999], "Computer Crime and Abuse: A Survey of Public Attitudes and Awareness." Computers & Security, 18(8), pp. 715-726.

Forcht, K. A. [1994], "Computer Security Management." Boyd Fraser Publishing, Massachusetts. (FO).

Hinde, S. [2000], "Smurfing, Swamping, Spamming, Spoofing, Squatting, Slandering, Surfing, Scamming and Other Mischiefs of the World Wide Web." Computers & Security, 19(4), pp. 312-320.

Jamieson, R and K. Stevens [2001], "INFS5984 – Information Systems Security Course Outline." School of Information Systems Technology and Management, the University of New South Wales, Sydney, 2001

Kelley, J. [2000], "Business Continuity: Battling High-Tech Exposures." Risk Management, May 2000, pp. 31-33.

Kravitz, P. M. and A. Pugliese [2000], "Lawmakers tackle privacy." Journal of Accountancy, June 2000, pp. 29-33.

Liu, S. and M. Silverman [2000], "A Practical Guide to Biometric Security." IT Professional 3(1), pp. 15-26.

Matyas, S. M. Jr., and J. Stapleton [2000], " A Biometric Standard fro Information Management and Security." Computers and Security 19(5), pp. 428-441

McKenzie, W. and D. Murphy [2000], "I hope this goes somewhere: Evaluation of an online discussion group." Australian Journal of Education Technology 16(3), pp. 239-257

Microsoft Corporation [2000], "Windows 2000 Distributed Security Features." Microsoft Technical Paper 2000 (www.microsoft.com)

Newman, D. and S. Rao [2000], "Regulatory Aspects of Privacy and Security - A View from the Advanced Communications Technologies and Services Programme." Information & Communication Technology Law 9(2), pp. 161-166.

North, K. [1999], "Web databases: Fun with guests or risky business?" Web Techniques 4(3), pp. 24-28.

Nosworthy, J. [2000], "Implementing Information Security in the 21st Century - Do You Have the Balancing Factors." Computers & Security 19(4), pp. 337-347.

Pangalos, G., C. Frangakis and S. Katsikas [1994], "Implementing database systems security." Computer Security Journal 10(2), pp. 73-99.

Richards, K. [1999], "Network Based Intrusion Detection: A Review of Technologies." Computers & Security 18(8), pp. 671-682.

Shaller, D. [2000], "E-mail the Internet and other legal and ethical nightmares." Strategic Finance, August 2000, pp. 48-52.

Standards Australia [2000], "AS/NZS 7799.2.2000, Information Security Management, Part 2: Specification for information security management systems", Standards Australia, March 2000.

Standards Australia [2001], "HB 231:2000, Information Security Risk Management Guidelines", Standards Australia, 2001

van Krugten, P. and M. Hoogenboom [2000], "B2C Security - Be Just Secure Enough." Computers and Security 19(4), pp. 348-356.

von Solms, B. [2000], "Information Security - The Third Wave." Computers & Security 19(7), pp. 615-620.

Wenninger, J. [1999], "Business-to-Business Electronic Commerce." Current issues in Economics and Finance 5(10), pp. 1-6.

Zviran, M. and W. Haga [1999], "Password Security: An Empirical Study." Journal of Management Information Systems 15(4), pp. 161-185.

AUTHOR BIOGRAPHIES

Kenneth Stevens is a lecturer in the School of Information Systems Technology and Management at the University of NSW where he teaches and researches in the fields of information systems security and audit. He holds a Masters of Commerce from the University of New South Wales – Sydney, and a Bachelor of Financial Administration from the University of New England – Armidale. His special research interest in is software development project risk and is applying risk management theory to this area. He is a Chartered Accountant with a background in IT consulting

Rodger Jamieson is director of SEAR (Security E-Business Assurance Research Group) and Associate Professor in the School of Information Systems, Technology and Management at The University of New South Wales. He holds a PhD, a Masters of Commerce (Honours) and Bachelor of Commerce (Honours) from the University of New South Wales – Sydney. He is actively engaged in research, and has published, in areas of IS security, IS auditing, computer forensics, electronic commerce and knowledge-based expert systems. He is a Chartered Accountant, a member of the Australian Computer Society and a member of the Information System Auditor and Control Association (USA). His prior work experience involves IS audit management with Touche Ross & Co. and Coopers & Lybrand.

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096