Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

Developing the Cross-Disciplinary Nature of Information Assurance in the Undergraduate Curriculum

Dr Jill Slay

Abstract — This paper responds to issues raised by Information Assurance (IA) researchers and teachers, ([1], [2], [3]) on the cross-disciplinary nature of the field. It seeks to expand the debate on the content of forensic computing, information security and information warfare curriculum by proposing a minor stream (or track) in Information Assurance which could serve as part of a broad range of undergraduate programs. These include degrees in science, social science or business rather than the technical ones, such as computer science and IT, where the IA minor stream is currently located.

Index Terms—Forensic Computing; Information Warfare; Information Security; Information Assurance; Undergraduate Curriculum

I. Introduction: Current Situation

The nature of the IA curriculum in higher education is continually under development. This is particularly apparent with the move towards the widespread incorporation of Forensic Computing within the undergraduate curriculum in Australia.

In previous work [4] the author has noted that it is difficult to establish general trends in the teaching of Information Assurance or IT Security in Australia. Nearly all Australian universities seek to accredit their IA curricula with the Australian Computer Society (ACS) and so these curricula have to meet the basic requirements set by ACS. These requirements are well-defined but may be treated fairly minimally and this may mean that security issues are covered technically within networking or software engineering or professional ethics courses and so there may be no evidence of a discrete IA course in the curriculum. A few universities do teach fairly substantial streams in IT or IS security but there is no evidence that the curriculum design in these cases is planned to cover any specified body of knowledge. One or two institutions draw on proprietary technology-based certifications as a foundation, for example, for their network security course and thus can offer industry accepted certification but there is no evidence that such courses are planned systematically to develop a well-established body of knowledge. The issue we have to face then in curriculum design, and in our teaching, is the one of attempting to produce rounded university graduates who think broadly about the wider issues involved in IA

II. What is missing from Current curriculum?

The content listed by the ACS is one which is fairly traditional in its approach to IT Security within a typical computer science curriculum. Current constraints on curriculum content prevalent in Australia when an IA course is contextualized within Computer Science or IT are listed below

Content must include [5]:

- Historical Background
- Societal, Governmental and Legal Imperatives for Information Systems Security and Privacy
- Professional Responsibility and Information Systems Security
- Computer Security
- Access control, Authentication, Integrity, Confidentiality
- Security Technologies
- Network Security
- Trusted Systems and Networks
- Concepts of security functionality and enforcement/verification
- Verification techniques and software engineering
- Security in the Distributed Systems (Client/Server) and Object Oriented Environments
- Security and Specific Industry Requirements
- Security Management

Other approaches to the issue of curriculum content which the author has taken in previous work [6] include that of suggesting that it is possible to map current IEEE, ACM and ACS expectations to the ISC^2 Common Body of Knowledge and thus teach:

1. Security Management Practices
2. Security Architecture and Models
3. Access Control Systems & Methodology
4. Application Development Security
5. Operations Security
6. Physical Security

ISBN 1-933510-99-4/05/$15.00

7. Cryptography
8. Telecommunications, Network, & Internet Security
9. Business Continuity Planning
10. Law, Investigations, & Ethics.

Taking the approach of teaching both the ACS and ISC^2 bodies of knowledge has served well for more than three years, but we have found there are enormous difficulties in taking a broad approach to curriculum when teaching IA concepts to computer science, software engineering or information technology students. Major issues include:

- A large number of our students, more than 60% of our current enrollment, have English as a second language and are only expected to be in our country for the 3 or more years it takes to complete their studies. They, along with many native born Australians of a wide range of ethnic backgrounds, have chosen to study Computer Science courses since these require little formal written assessment and, in many cases, have not been prepared in their previous technical studies for the quantity of reading required to master IA concepts. Even more importantly they have not been taught broader 'liberal arts' concepts such as critical thinking and textual analysis which may be required. If such students are to succeed and then to embark on a research path in IA, they need enormous learning support and the development of skills such as academic reading, writing, note-taking, time management and referencing.
- Similarly a large number of our students live in, or will return to, countries where employability in areas such as Forensic Computing is minimal or where law, ethics and constitution (e.g. China) are constructed in a manner which is very different to that of USA, UK or Australia. So there is some question as to whether learning detailed investigative techniques based on Australian legislation are very useful.
- A similar argument can be made too about industry needs in the wide range of countries from where we draw our international students. While we can develop clear agreement on the technical development of countries such as Singapore and Hong Kong SAR, we can only really depend on the expressed hopes and ambitions of the less-developed world so it is hard to teach truly relevant curriculum in some case
- Many students join our 3 and 4 year undergraduate programs with academic credit gained from Diploma studies in SE or S. Asia. The presumed prerequisites are sometimes non-existent and so we need to teach the basics of networking, hardware and operating systems as well as, in some cases object-oriented programming.

III. Developing a New Approach

Research in the foundations of Forensic Computing, which in many ways mirrors the foundation of the whole of Information Assurance, has shown the cross-disciplinary nature of Forensic Computing.

In previous work [6] we noted that among researchers and practitioners there is a lack of an overarching conceptual framework within which to place Forensic Computing in particular, and here by extrapolation Information Assurance in general. This lack of a 'pure' disciplinary framework was identified by Broucek &Turner [7] as a source of both confusion and frustration for researchers wishing to explore aspects of the emerging discipline of forensic computing. They saw that practicing police and forensics computing investigation teams rely on individual members contributing a variety of knowledge, skills and experience in order to provide all the necessary human resources to undertake Forensic Computing Investigations. They produced taxonomy of forensic computing skills to provide both the academic community and practitioners within the field of Forensic Computing a basis for examining existing research and skills and upon which to direct research for the future development of practitioner knowledge, skills and experience.

Their taxonomy suggests that Forensic Computing includes

- **Computer Science:** Operating Systems and Application Software, Systems Programming and Programming Languages,
- **Computer Security,**
- **Computer Law** (national and international), Criminal, Civil and Soft Law
- **Information Systems**: Systems Management and Policies, User Education and Training
- **Social Science**: Socio-political issues (privacy, encryption, surveillance), Activism, Hacktivism, Cyberterrorism and Cyber-warfare, Socio-psychological impacts of computing

Broucek and Turner [7] indicated that this taxonomy illustrates the breadth and depth of issues of relevance to Forensic Computing research, illustrates the multiple perspectives which must be taken and overcomes the common misconception that Forensic Computing is just a new name for computer security. They also concluded that any coherent Forensic Computing research framework must therefore acknowledge:

- **National and organisational cultural** differences in the focus of approaches: individual, organisational, national and supranational;
- **Differences in the scale of systems:** personal computer and other individual devices;

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

intranet; extranet, VPN and the Internet.

If we extrapolate Broucek and Turner's [7] work we find we have a model for undergraduate curriculum and, with clever design, can imagine a stream of six courses which might easily be taught to students other than those in computer science and software engineering (who would, of course not be excluded) to those who have foundations in basic High school mathematics and science and some English and social studies

IV. The Effect of the need for Forensic Readiness and or Information warfare on IA curriculum

Other social and political issues beyond the research of Broucek and Turner [7] which point to the growing need for Information Assurance, and particularly Forensic Computing awareness flow out of the need for good Corporate governance which has grown out of the development of Sarbanes – Oxley and similar European Legislation

Law enforcement investigators have a very good understanding of the computer and network data which needs to be provided to them by an organisation in the case of forensic investigation, based on their knowledge of law, and the functionality of the most commonly used forensic investigation tools. These investigators can then produce robust software-generated reports as evidence which can stand up in a court of law. However they are hampered in this work because Australian enterprises are not aware that they should collect computer and network data, log files and records in a systematic manner. This means that when a system breach occurs, or computer crime is suspected, the potential evidence is not available for law enforcement investigators to analyse, and in some cases has never been collected.

We can train computer scientists to develop good forensic software and we can also train the few forensic analysts Australia needs within the university. However we are failing to educate business and commerce graduates with any concept of forensic readiness as apart of a more comprehensive IA program.

Rowlingson [8] defines forensic readiness as 'the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation.' This definition relies on an organisation systematically and routinely collecting all necessary data to supply the forensic investigative process, and thus produce evidence which is admissible in court.

Currently the IT management, and particularly the security management, of Australian organisations is largely governed by a series of national and international standards which are based on process models created before the widespread growth of computer crime. These models do not incorporate an awareness of the need for organisations to prepare for computer crime, and do not focus on the need to design systems which are able to produce digital evidence which is forensically sound and able to be presented by police and other law enforcement agencies in a court of law. Such awareness and sound design is termed 'forensic readiness' [8].

The Sarbanes Oxley Act of 2002 has been enacted in the USA to deal with cases of business crime and poor corporate governance which had resulted in the Enron affair and other recent notorious cases of corporate crime. This act establishes corporate responsibility to create proper processes which allow a quick response to potential fraud. Companies have to establish controls which allow 'prevention, identification and detection of fraud' through a series of 'internal controls'. The ability to collect, verify and store computer evidence is a very necessary and ongoing part of the establishment of the controls required by the Sarbanes-Oxley Act [9].

Similarly new standards for international banking were developed in Europe by the Basel Committee on Banking Supervision (known as Basel 2) in a report [10] focusing on the issue of the management of risk inherent in internet and electronic banking. Major actions featured in the report include a need for banks to prepare incident response plans and to identify processes to identify, 'collect and preserve forensic evidence to facilitate post-mortem reviews of any e-banking incident as well as to assist in the prosecution of attackers'. The report also firmly placed responsibility for this process on the shoulders of Boards of Directors and senior mangers of enterprises, making them responsible for risk management, security control processes and thus forensic readiness.

The implications of this US legislation and European standards for the Australian corporate sector are that all Australian companies working, or wishing to work, internationally will need to establish processes to collect verify and store computer evidence as part of their ongoing IT management processes, and that multinational companies working in Australia are already obliged to comply with this legislation. Australian enterprises therefore have a double obligation to understand and embed forensic readiness concepts within their own IT and security management processes. Australian Universities need to co-operate in this process by producing business, commerce and IS graduates who are aware of the intricacies of information systems, their security and the foundations of forensic computing.

This then points to a need for a basic IA stream in undergraduate business, commerce and IS degrees which includes:

- **Computer Science:** Operating Systems and Application Software, Systems Programming

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

- **Computer Security,**
- **Network Security**
- **Computer Law** (national and international),
- **Information Systems**: Systems Management and Policies

Hutchinson [2] also examined the issue of curriculum, at the postgraduate and masters level, in his search for a method of integrating 'intelligence' within IT Security to produce an effective Information Warfare curriculum
.
His approach is one in which 'is based on the assumption that the exploitation and protection of information (hence, knowledge and data) cannot be separated.'

He bases this approach on the following:

'In a modern organisation all functions (including the Information Security function) should be dynamically assisting the organisation to achieve information superiority
• The information security function is about human and data management (and their associated communication, storage and processing technologies), and
• The definition of 'information' used above is more akin to the conventional meaning of 'intelligence'.'

The outcome of his work is a postgraduate curriculum which includes technical and social science content in :

- **Database Security**
- **Computer Security**
- **Physical Security**
- **Fundamentals of Cyber-crime**
- **Media and Advertising)**
- **Media and Nation**
- **Media and Social Issues**
- **Ethics, Values and Moral Decision Making**
- **Current Issues in Security**
- **Advanced Security Risk Management**
- **Advances in Security Technology**

V. Conclusion: A Proposed Cross-Disciplinary Minor Stream in Information Assurance

The conclusion from a review of literature and an evaluation of academic practice in Australia is that there is an industry-based and social need to teach Information Assurance in disciplines other than Computer Science or Software Engineering. This curriculum can assume no technical prerequisites but does assume that the student comes from a background which is language rich and where knowledge will be applied in a social or business and commercial context.

This also assumes that there are many career and research outcomes in Information Assurance other than the pure computing ones our curriculum currently serves to meet.

Indeed this kind of approach would bring a richness to a field which is often ostrich-like in burying itself away from the social, legal, ethical and political outcomes of technology development and dependence which is currently inherent in our IEEE/ ACS/ ACM technically compliant approach.

A new curriculum certainly needs content based on some technical knowledge in computing but can afford to be wider in its integration of our domains:

Computer basics and security: Operating Systems and Application Software, Systems Programming, non-formal foundations of cryptography

Network and system basics and security: Network foundations (media and protocols, Network security basics (IDS, firewall, VPN),

With Broucek and Turner [7] the curriculum would include:

Law: national and international, Computer, Criminal, and Civil

Social Science: Socio-political issues (privacy, encryption, surveillance), Activism, Hacktivism, Cyberterrorism and Cyber-warfare, Socio-psychological impacts of computing

With Hutchinson some choice would be given within:

- **Physical Security**
- **Fundamentals of Cyber-crime**
- **Ethics, Values and Moral Decision Making**
- **Current Issues in Security**
- **Advanced Security Risk Management**

It would be appropriate to add more electives including:

- **Forensic Computing Investigation**
- **Forensic Computing Applications and Technology**

This curriculum would be appropriate to industry and to the protection of the Australian National Infrastructure.

However this curriculum solution may not be internationally appropriate given the difference in higher education and high school curriculum structur,e but is offered here as a considered Australian response to the need to develop Information Assurance beyond the Computer Science Curriculum.

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

VI. REFERENCES

[1] Yasinsac, A., Erbacher, R., Marks, D.G., Pollitt, M.M. and Sommer, P. (2003) Computer Forensics Education ,IEEE Security and Privacy, July 2003.

[2] Hutchinson, W. (2003) The Case for Integrating Information Security and Intelligence Courses. Wise 3, San Diego.

[3] Endicott-Popovsky, B., Popovsky, V.M. and Frincke, D. (2004) *Designing a Computer Forensics Course for an Information Assurance Track*,, 8th Colloquium for Information Systems Security Education, USMA WestPoint New York.

[4] Slay, J & Lock, P. (2005) *Developing An Undergraduate IT Security Stream*. Accepted for Wise 4 Moscow, May 18-20, 2005

[5] ACS. (n.d) Body of Knowledge, viewed online < http://www.acs.org.au/national/pospaper/bokpt3.htm#5.11> 17/11/05.

[6] Slay, J. (2004).*Embedding Industry Standards within the Undergraduate IT Security Curriculum: An Australian Implementation*, 8th Colloquium for Information Systems Security Education, USMA WestPoint New York.

[7] Broucek, V. & Turner, P 2001, Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare ,.*Journal of Information Warfare 1(2)*: 95-108.

[8] Rowlingson, Robert 2004, A Ten Step Process for Forensic Readiness, *International Journal of Digital Evidence (2:3)*, Winter 2004, pp 1-28.

[9] Patzakis, J 2003, New Accounting Reform for Technology-Based Document Retention Practices, *International Journal of Digital Evidence (2:1)*, Spring 2003, pp 1-8.

[10] Limongelli, V 2003, *Basel Committee Incident Response Standards, [*Online, accessed 5 Feb. 2005]. URL: http://www.guidancesoftware.com/corporate/whitepapers/downloads/BCIRStandards.pdf.

ISBN 1-933510-99-4/05/$15.00