HAL
archives-ouvertes.fr

Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula

Lynn Futcher, Johan Niekerk

▶ To cite this version:

Lynn Futcher, Johan Niekerk. Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula. 8th World Conference on Information Security Education (WISE), Jun 2011, Lucerne, Switzerland. pp.164-171, 10.1007/978-3-642-39377-8_18 . hal-01463616

HAL Id: hal-01463616
https://hal.inria.fr/hal-01463616

Submitted on 9 Feb 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

Proceedings of the 7th World Conference on Information Security Education
9-10 June 2011, Lucerne, Switzerland

Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula

Lynn Futcher[1] and Johan van Niekerk[2]

[1,2] Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
{Lynn.Futcher@nmmu.ac.za, Johan.VanNiekerk@nmmu.ac.za}

Abstract. Information Technology (IT) encompasses all aspects of computing technology. The pervasiveness of IT over the past decade means that information assurance and security (IAS) know-how has become increasingly important for IT professionals worldwide. However, South African universities do not get specific curriculum guidelines to ensure that all essential security-related aspects are included in the IT courses offered. With respect to IAS, these universities are therefore required to self-regulate through measuring against international norms and standards. One such norm for the IT profession is given by the ACM/IEEE-CS in the *'Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programs in Information Technology'* document. This paper examines this norm, together with relevant South African curricula policy document, to establish what information security guidance exists to support IT curriculum developers and educators. In addition, it argues that an integrated educational IAS model can help address IAS as a pervasive theme throughout IT curricula.

Keywords: Information security education, information assurance and security model, IT curriculum

1 Introduction

Over the past decades, four major organizations in the United States have developed computing curricula guidelines for colleges and universities. These include the Association for Computing Machinery (ACM), the Association for Information Systems (AIS), the Association for Information Technology Professionals (AITP) and the Computer Society of the Institute for Electrical and Electronic Engineers (IEEE-CS).

The School of Information and Communication Technology (ICT) at the Nelson Mandela Metropolitan University (NMMU) is responsible for educating Information Technology (IT) professionals for tomorrow. However, it does not get specific curriculum guidelines to ensure that all essential security-related aspects are included in the IT courses offered. The South African curricula guidelines for IT qualifications

[1,2,3,4] dictate the instructional offerings which need to be incorporated at each level of the curricula. However, they do not provide in-depth guidance with respect to recommended content. As a South African university, the NMMU is therefore required to self-regulate through measuring against international norms and standards. One such norm for the computing profession is provided by the ACM/AIS/IEEE-CS Computing Curricula 2005 [5]. More specifically, such a norm for the IT profession is offered by the ACM/IEEE-CS in the '*Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programs in Information Technology*' document [6].

The purpose of this paper is to argue that the ACM/IEEE-CS and the South African Council for Higher Education (CHE) curricula guidelines do not provide sufficient guidance to **ensure** that information security is adequately incorporated within the IT curricula of the School of ICT, NMMU. In addition, it proposes an integrated IAS educational model to help address IAS as a pervasive theme throughout IT curricula.

The following sections discuss these guidelines and the extent to which they support IT curriculum developers and educators at South African universities. This is followed by some critical comments and recommendations in this regard.

2 ACM/IEEE-CS Curriculum Guidelines for Undergraduate Degree Programs in Information Technology

IT is the latest academic discipline covered by the ACM/AIS/IEEE-CS Computing Curricula volumes [5,6]. According to ACM/IEEE-CS, the pillars of IT include programming, networking, human-computer interaction, databases, and web systems. These are built on a foundation of knowledge of the fundamentals of IT. Overarching the entire foundation and pillars are information assurance and security, and professionalism [6].

The ACM/IEEE-CS's '*Information Technology 2008, Ccurriculum Guidelines for Undergraduate Degree Programs in IT*' [6] presents a curriculum for a 4-year study in IT. In so doing, it defines an IT body of knowledge that spans 13 knowledge areas. Information Assurance and Security (IAS) is one of these knowledge areas. These knowledge areas are further divided into smaller units, each of which represents individual themes within the respective areas. At the lowest level of the hierarchy, each unit is subdivided into a set of relevant topics.

IAS as a knowledge area is well defined by the ACM/IEEE-CS [6] curricula guidelines. It is recognised as a very integrative knowledge area and one in which all senior IT students should be involved. ACM/IEEE-CS specifically states that '*every student should be involved with some of the advanced security outcomes*' and that '*every student needs some advanced, integrative experience in IAS* ***in the 4th year'***. As a knowledge area, it is divided into various units including *Fundamental Aspects*, *Security Mechanisms*, *Operational Issues*, *Policy*, *Attacks*, *Security Domains*, *Forensics*, *Information States*, *Security Services*, *Threat Analysis Model* and *Vulnerabilities*. Approximately 7.5% of the total core hours defined for the 4-year curriculum should be allocated to IAS. However, since much of the content listed by IAS as a knowledge area may be regarded as primarily aimed at 4th year level, there is

a concern that some university curricula may only address security-related issues at this level. In addition, at some universities it may be regarded as an elective since it is a specialized field of study.

The ACM/IEEE-CS [6] addresses this concern to a certain extent since various security units and topics are defined within other knowledge areas. In general, the knowledge areas of IT Fundamentals (ITF), Information Assurance and Security (IAS), Information Management (IM), Integrative Programming and Technologies (IPT), Networking (NET), Platform Technologies (PT), System Administration and Maintenance (SA), Social and Professional Issues (SP) and Web Systems and Technologies (WS) all address some aspects of information assurance and security. For example, software security practices lies within the Integrative Programming and Technologies (IPT) knowledge area and a security unit is defined for the Networking (NET) knowledge area. In addition, Vulnerabilities is listed as a unit within the Web Systems and Technologies (WS) knowledge area. However, the knowledge areas of Human Computer Interaction (HCI), Mathematics and Statistics for IT (MS), Programming Fundamentals (PF) and System Integration and Architecture (SIA) contain no security-related aspects.

ACM/IEEE-CS [6] also addresses IAS as a pervasive theme as discussed in the following section.

3 IAS as a Pervasive Theme

In addition to having been defined as a key knowledge area, IAS has also been defined as a pervasive theme. ACM/IEEE-CS [6] describes a pervasive theme as those topics which are '*considered essential, but that did not seem to belong in a single specific knowledge area or unit'*. These themes should therefore be woven into the curriculum by being addressed numerous times and in multiple classes [6]. The pervasive themes of the IT curriculum are described under IT Fundamentals (ITF). The ACM/IEEE-CS [6] states that all the IT pervasive themes be covered by the end of the 4-year curriculum and that they must be addressed frequently from 1st to 4th year. However, although IAS is defined as both a knowledge area and a pervasive theme, at some universities it may be overlooked until the 4th year.

According to the IT body of knowledge, as defined by the ACM/IEEE-CS [6], IT Fundamentals (ITF) should take up approximately 8% of the core hours as indicated in the IT curriculum. Of this 8%, '*Pervasive Themes in IT'* should present approximately 68% which equates to roughly 5.5% of the total core hours defined for the 4-year curriculum. However, no further breakdown is provided as to how much time should be allocated to IAS as a pervasive theme. This means that other topics within the '*Pervasive Themes in IT*' unit may be given preference over IAS. This may lead to an IT graduate leaving university with apparent gaps in their security-related knowledge.

According to the IT curricula guidelines of the ACM/IEEE-CS [6], the IT Fundamentals (ITF) knowledge area is intended to be at the introductory level in a curriculum. The purpose of the ITF knowledge area is to develop fundamental skills for subsequent courses by providing an overview of the IT discipline and how it

relates to other disciplines. In so doing, it should instill an IT mindset that helps IT students understand the diverse contexts in which IT is used [6].

The ITF knowledge area is divided into four units. These units include '*Pervasive Themes in IT*', '*History of IT*', '*IT and its Related and Informing Disciplines'* and '*Application Domains'*. IAS is further listed as a topic within the '*Pervasive Themes in IT*' unit. Linked to IAS as a topic is the core learning outcome which is stated as - '*Explain why the IAS perspective needs to pervade all aspects of IT*'.

Many South African universities use these guidelines provided by ACM/IEEE-CS as an informal reference when creating IT curricula. However, it is the opinion of the authors that these guidelines do not adequately address IAS as a *pervasive* theme and that no further guidance exists to assist IT educators in developing curricula to ensure that IAS is effectively integrated into the curriculum at undergraduate level. In support of this argument, Futcher, Schroder and Von Solms [7] question the extent to which information security is incorporated into the IT/IS/CS curricula at South African universities. They raise the concern that information security is not being addressed adequately at undergraduate level and suggest that information security be defined as a critical cross field outcome (CCFO) in South African curricula guidelines. This implies that security-related aspects be integrated into the IT/IS/CS curricula from the 1st year of study. In line with this, the following section provides a critical evaluation of current South African curricula guidelines [1,2,3,4] against the ACM/IEEE-CS [6] guidelines.

4 A Critical Evaluation of South African Curricula Guidelines Against the ACM/IEEE-CS

The South African Council for Higher Education (CHE) provides guidance to tertiary institutions regarding curriculum composition. This guidance currently resides in documents from the Higher Education Qualifications Framework (HEQF), the South African Qualifications Authority (SAQA) and the National Assembly Training and Education Department (NATED). This section examines the guidance provided by the CHE specific to IT qualifications [1,2,3,4] in order to critically evaluate it against the ACM/IEEE-CS [6] curriculum guidelines. The aim is to identify possible weaknesses and areas for improvement with respect to integrating information security into IT curricula.

The HEQF is a qualifications framework for a single coordinated higher education sector. It applies to all higher education programmes and qualifications offered in South Africa by public and/or private institutions. As such, it replaces previous policy documents including '*A Qualification Structure for Universities in South Africa - NATED Report 116 (99/02)'*, '*General Policy for Technikon Instructional Programmes - NATED Report 150 (97/01)'* and the '*Formal Technikon Instructional Programmes in the RSA - NATED Report 151 (99/01)*'. However, some relevant curricula information still resides in the NATED documents.

The NATED Report 151 specifies instructional offerings for a National Diploma [2] and Bachelor of Technology in Information Technology [1]. Although no specific security-related offerings are stipulated for the National Diploma [2], Computer

Security IV and Information Security IV are specified for the Bachelor of Technology [1] qualification. However, these two offerings are not compulsory in any of the nine specialised IT fields as defined by SAQA [3,4]. These IT fields include Business Applications, Software Development, Communication Networks, Web and Application Development, Information Systems and Technology Management, Intelligent Industrial Systems, Support Services, Technical Applications and Hardware and Computer Architecture.

None of these IT fields have any security-related exit level outcomes nor specific outcomes identified for the SAQA registered National Diploma in IT [4]. For all nine IT fields, the SAQA registered Bachelor of Technology in IT qualification [3] defines a security-related exit level outcome that states that '*the qualifying learner should have the ability to apply advanced techniques in the introduction and control of information security in an IT environment*'. However, this is only stipulated as being core for the Business Applications field and as an elective for the other eight IT fields. Linked to this exit level outcome is the associated assessment criterion '*Evaluate the information security environment and design control measures'*. This poses a major concern with respect to addressing IAS as a pervasive theme within South African IT curricula.

In comparison, the ACM/IEEE-CS's curriculum guidelines [6] offers an excellent baseline from which to develop a 4-year IT curriculum. Specifically, at the 4th year level it recommends the inclusion of IAS as an advanced subject area and it provides very clear guidelines on the topics such an instructional offering should be covering [6]. However, specific guidance on *how to* incorporate security concepts as a pervasive theme during the first three years of study, and as part of the remaining 4th year subjects, is lacking.

This could lead to potential problems at several different levels. Firstly, the structure of the 4-year IT curriculum at the NMMU, and several other similar South African universities, is such that the 4th year of study forms part of an optional, more advanced, qualification [1]. It is thus possible for a student to exit the qualification after the 3rd year of study. Secondly, even for students who do decide to enroll in the optional 4th year qualification, the "Information Security" instructional offering is not considered compulsory in the South African curriculum guidelines, and is thus an elective subject [1]. Students could thus elect to not receive the requisite information security education. This means that the lack of *specific* guidance on how information security-related concepts should be incorporated *as a pervasive theme* into the curricula of subjects during the first three years of study could lead to IT curricula that do not adequately address information security, despite the relative importance assigned to this topic by the ACM/IEEE-CS's [6] curriculum guidelines.

Even though it cannot reasonably be expected from the ACM/IEEE-CS to provide subject specific guidance on these topics, it could be argued that a minimum "standard" for each topic area could be more clearly delineated by the curricula guidelines. Such delineation could possibly be done with the assistance of the information assurance model suggested in the ACM/IEEE-CS guidelines [6], to provide the context for information security knowledge, and the use of a learning taxonomy like Bloom's taxonomy, as suggested by Van Niekerk & Von Solms [8] to provide guidance on the "depth" of topic coverage at a specific year of study.

As an example it could be argued that the topic of "buffer overflow attacks/prevention" should not simply be relegated to form part of an *optional* 4th year subject. Instead it should be integrated into programming subjects throughout the qualification. Thus, with the help of a learning taxonomy, like Bloom's, specific learning objectives could be defined which requires learners at the 1st and 2nd years of study to **remember** and **understand** material relating to this topic, and which requires 3rd year students to be able to **apply** the relevant knowledge.

This integration of the topic into the programming curriculum could also provide security context through the incorporation of the suggested information assurance model. Relevant topics could thus still refer to the underlying information states, security services and/or security countermeasures relevant to the context in which these topics are being taught. Table 1 provides brief examples of sample learning activities for the topic of "buffer overflow attacks/prevention" for the lowest three levels of Bloom's taxonomy only. Similar examples could also be constructed for the remaining levels but were omitted due to space constraints.

Table 1. Abbreviated example of Learning Activities based on Bloom's Taxonomy for Information Security, adapted from Anderson, et al. [9].

Level	*Verb*	*Sample Activities*
Apply	execute	Write error prevention code to ensure that your methods iterating through the given list of stored items cannot overstep the boundaries of this list. (Security Countermeasure)
Understand	discuss	Explain how the integrity of the data in the computer's memory could be negatively affected if your code tries to access an array element outside the boundaries of the current array. (Security Services)
Remember	define	In terms of the underlying memory used/allocated, define what an array of 32 bit integers is. (Information States)

The information assurance model suggested by ACM/IEEE-CS [6] can also be adapted to reflect this incorporation of Bloom's taxonomy into the intended curriculum design process. Such an adaptation is illustrated in Figure 1. This is similar to an earlier adaptation by Maconachy, Schou, Ragsdale & Welch [10], where "Time" was added as a fourth dimension to the model. The addition of a time dimension was not used as "*a causal agent of change, but a confounding change agent*" [10]. This catered for the need to modify other dimensions to cater for new technologies which are introduced over time.

The adaptation depicted in Figure 1 similarly is not a causal agent, but rather serves to illustrate the increasing "depth" of the student learner's mastery of the underlying, pervasive security concepts, in terms of Bloom's taxonomy, as such a student progresses through his/her studies. A student might therefore initially only deal with a specific concept at the "remember" dimension of the cognitive domain but should, over time, progress towards the "create" dimension.

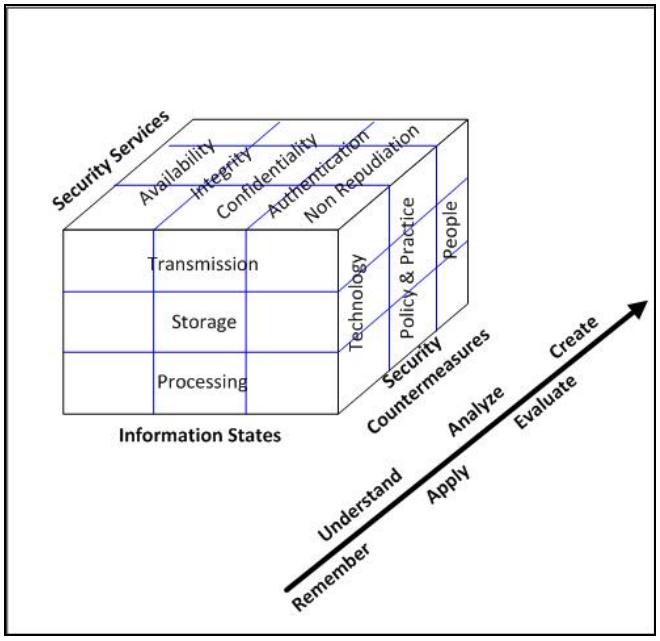

Figure 1: Model for Pervasive Information Assurance and Security Education (adapted from Maconachy, Schou, Ragsdale, Welch [10])

Weaving many of the IAS concepts into the curriculum provides challenges unique to the IT profession. It is this challenge which this proposed model for pervasive information assurance and security education, as depicted in Figure 1, could help to address.

5 Conclusion

Although the ACM/IEEE-CS advocates IAS both as a knowledge area and as a pervasive theme, there is little guidance provided with respect to assisting IT educators in incorporating information security as a pervasive theme into their various offerings. More guidance should be given by either the ACM/IEEE or at national level with respect to IAS as a pervasive theme. In order to integrate IAS pervasively into IT curricula, it would be sensible to use a learning taxonomy to "phase in" concepts. By utilizing the proposed pervasive information assurance and security model for IT education, curriculum developers and educators can determine the fundamental, core and elective security-related aspects to be incorporated from the 1st to the 4th year of the IT qualification. Whereas fundamental aspects should form the essential basis required for the proposed qualification, core aspects should include the compulsory learning required in situations contextually relevant to the particular

instructional offering. Elective aspects should include any additional optional security-related aspects that could enhance the qualification. Incorporation of the proposed model could benefit the guidelines provided by both the ACM/IEEE-CS and the CHE.

Finally, CHE does not provide detailed subject level guidelines. It is the authors' opinion that IT educators in South Africa could benefit from formally adopting ACM/IEEE-CS guidelines since extensive guidance is provided. However, from a security perspective the authors believe that even more guidance specific to the incorporation of security as a **pervasive** theme is needed. However, future research is required to determine whether security-related aspects are specified within institutional learning programme guidelines.

References

1. South African Council for Higher Education (CHE) (2005). NATED DOCUMENT 151: BACCALAUREUS TECHNOLOGIAE: INFORMATION TECHNOLOGY.

2. South African Council for Higher Education (CHE) (2005). NATED DOCUMENT 151: NATIONAL DIPLOMA: INFORMATION TECHNOLOGY.

3. South African Qualifications Authority (SAQA) (2007). REGISTERED QUALIFICATION: Bachelor of Technology: Information Technology. http://regqs.saqa.org.za

4. South African Qualifications Authority (SAQA) (2007). REGISTERED QUALIFICATION: National Diploma: Information Technology. http://regqs.saqa.org.za

5. ACM, AIS & IEEE-CS (2005). Computing Curricula 2005: The Overview Report.

6. ACM & IEEE-CS (2008). Information Technology 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology.

7. Futcher, L.; Schroder, C. & Von Solms, R. (2010). Information security education in South Africa. Information Management & Computer Security. Vol 18, No. 5. pp 366-374.

8. Van Niekerk, J., & Von Solms, R. (2009). Using Bloom's taxonomy for information security education. Education and Technology for a Better World. 9th IFIP TC 3 World Conference on Computers in Education, WCCE 2009, Bento Goncalves, Brazil, July 2009.

9. Anderson, L., Krathwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., Raths, J., Wittrock, M. (2001). A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Complete Edition. Longman.

10. Maconachy, W. V., Schou, C. D., Ragsdale, D. & Welch, D. (2001). A Model for Information Assurance: An Integrated Approach. Proceedings of the 2001 IEEE workshop on IAS, United States Military Academy, West Point, New York, June 2001.