30

IT Security and Privacy Education

Louise Yngström
Department of Computer and Systems Sciences, Stockholm University and Royal Institute of Technology, Electrum 230, S-164 40 Kista, Sweden
voice 46-8-16 16 10, fax 46-8-703 90 25, email louise@dsv.su.se

Abstract

An ever repeated problem within IT security is awareness and understanding. Some think this is due to failing educational systems and will be solved by interdisciplinary courses and programmes. This paper gives and overview of new developments within university education in IT Security, and analyses in particular what is meant by interdisciplinary approaches. An overview of existing models and frameworks for building educational programmes is given, and the most evident new directions for educators are outlined.

Keywords

IT Security education, teaching strategies, educational frameworks

1 INTRODUCTION

First I must thank the organisers for inviting me to talk on my favourite topic. As many of you know, I regard education a very important issue in our endeavours to create a safe, secure, just, humane, and global Information Society. And one way to catch everybodys concerns and interests is to start with privacy. Whatever our definition of the concept and whatever our original culture, we all have a notion of privacy as a fundamental physiological need and familiar cultural construct (Lunheim and Sindre 1994). And whenever privacy is mentioned in relation to IT people have an opinion.

The same is however not true for security. Security as such is such a difficult concept! Although most important communications on security: discussions, papers, text books, research and developments, etc. are presented in English, most of us have other mother tongues. In many European languages such as German, Swedish, French, Spanish, and Italian safety and security are included in the very same concept (Burns, McDermid and Dobson 1992) and in Greek security, safety, insurance, and assurance all call for the same concept: asfalia. No wonder it is a difficult task to make people understand what we mean. In this context education is an important mean to harmonise and smooth over cultural differences.

S. K. Katsikas et al. (eds.), *Information Systems Security*

The original reason for me to start university courses in IT Security was exactly my interest in privacy in relation to computer systems, and the educational challenge of making aspects of IT Security comprehensive to managers and security managers. Kristian Beckman, the founder of TC11 and the chairman of the Educational Committee of the Swedish Vulnerability Board, introduced me to the vast societal needs of knowledge, understanding, and good practices of IT Security. The specification of our first university programme was the result of discussions, a lengthy correspondence, and participation in Kristian's project 'The Swedish Tiger' - the first textbook in Swedish on IT security (RDF 1986).[1] We specified the educational programme from the envisaged needs of the users, the organisations, and society - following the Scandinavian tradition of user oriented system analysis.

It felt natural in Sweden to take that approach. Our privacy legislation in 1973 had been preceded by great interest in the media and people in organisations, at least in management positions, were aware of the problems involved and looking for solutions.

2 TWO APPROACHES TO IT SECURITY AND PRIVACY EDUCATION

In addition to the user oriented approach, often labelled the interdisciplinary approach, because it has to incorporate at least economic, legal, social, and ethical aspects, there is the traditionally disciplinary oriented specialist approach. The latter is today the rule, although there have been, for some time now, strong demands for interdisciplinary oriented programmes on postgraduate levels (National Research Council 1991) and for taking account of political, cultural, social, commercial, and technical needs for the definition, development, positioning, management, implementation, and use of infosec controls (INFOSEC 1992).

2.1 Epistemological pluralism

Before I go any further, let me underline this: some educators seem to think interdisciplinary courses are easy (to pass) while disciplinary courses are more difficult (to pass). I think neither is true. Both of them can be easy or difficult; it is rather a matter of matching learning and teaching styles - apart from incorporating or excluding knowledge from other disciplines.

Interesting tests in mathematics education have show that school pupils with a traditional learning style (learning concepts from investigating details) offered education through an untraditional teaching style (teaching about details from concepts) performed as badly in tests as school pupils with an untraditional learning style offered traditional educational style. When matching learning and teaching styles correctly, both groups performed as well (Siklossi 1966). Sherry Turkle (1990) interprets this as demands for epistemological pluralism. She shows how technological developments has led to possibilities for using and controlling the computer - specially within learning and education - in different ways. Neither way is more 'right' or 'better' than the other, but instead an effect of different conceptualisations or styles. Students who prefer the untraditional learning mode, called bricoleurs after Claude Lévi-

[1] the English translation of this project calls for a short explanation: 'The Swedish tiger' was during WW2 used as a code, with 'tiger' having the double meaning of the animal and to 'keep quiet'. Posters with the tiger reminded the Swedes about keeping information confidential. To have a short and associative title, members of the project suggested to reuse the code and the cover page shows a tiger walking on sheets of printouts.

Strauss (1968), construct theories by arranging and rearranging, by negotiating and re-negotiating with a set of well known materials, but the result of their work is as organised as if an ordinary structured approach would have been used. So it is not a difference of end products between bricoleurs and traditional learners but a difference of processes leading to the end result. By accepting and opening for epistemological pluralism we would accept the validity of multiple ways of thinking and learning - as well for disciplinary as interdisciplinary programmes and courses.

However, I believe interdisciplinary courses in our subject more often use untraditional teaching strategies because parts of the other needed disciplines incorporate types of knowledge that we usually do not deal with.

Martin and Holz (1992) has found that for successfully teaching areas such as ethics within a computer science curriculum, a framework which can incorporate personal, social, and professional values is needed. Aided by this framework, the student can investigate, in different ways, the actual outcomes of chosen value theories in combination with stated professional practices and codes of conduct. The result looked for is a meta-framework for personalised decision making , although the learning processes involved could be very varied.

Similarly, the ImpactCS Project (1995) finds teaching ethics atypical to computer science, because "We can quantify the complexity of a procedure, but this quantification by itself does not resolve the need for a judgement of the risk involved in using that procedure in a particular application. We can mathematically describe the state of a machine, but if we want to make claims about its effectiveness in use, we also need to understand the situation in which that machine will be used. Thus the actual practice of computing involves judgements about *computers in use*, and these judgements require knowledge and skill in the ethical and social context of computing." (p 1).

Although the differences between involved disciplines, Miller (1988, p 37) notes: "...societal and technical aspects of computing are interdependent. Technical issues are best understood (and most effectively taught) in their social context, and the societal aspects of computing are best understood in the context of the underlying technical detail."

Within engineering oriented university education we tend to use the traditional oriented teaching style more often, and those students who do not fit will leave. Moreover, interdisciplinary courses and programmes are not favoured by most research oriented university departments.

When the environment now demands interdisciplinary approaches because there are needs for more knowledgeable persons, these demands could be interpreted both as quests for widening the scope of what we are teaching and quests for paying attention to learning styles. Thus we should add these new structures and methodologies rather than throw away what we have.

And I think this is what is emerging: there is as well a starting movement towards interdisciplinary programmes and courses as an increase of specialised courses and programmes on undergraduate and postgraduate levels. And there are efforts to construct more and varied student oriented material to substitute and complement traditional teaching.

2.2 Current trends within IT security education

A study by Higgins (1989) in US showed that 25 out of 102 departments offered 31 courses in computer security, mostly on advanced undergraduate or graduate levels. Most courses were taught by computer science departments (25) while two courses were offered by departments of mathematics and one each by departments of management, business, accounting and administrative sciences. The same phenomena is also evident in Europe; most programmes and courses started on research level in departments of computer science or mathematics. However in the 1990ies there is a shift towards offering courses and programmes on undergraduate and master levels; European surveys (Gritzalis 1995, Yngström 1995b) show an increasing amount of courses in computer security as a part of a standard bachelor curriculum in Computer Science and there is a move towards master curricula in Information Security. This is also evident for North America and Australia, although no detailed surveys of these countries have been found or conducted.

There are still fewer interdisciplinary approaches than specialised, at least when it comes to separate courses. Typically courses in an undergraduate programme extends to 1/8 of an academic year (equivalent of 7,5 European Credit Transfer System points or 3 US academic credits) and includes, when strictly technical, cryptology, operating systems security, security models and evaluation models. Interdisciplinary labelled courses add managerial, legal, ethical, and social issues. Interdisciplinary courses are often taught partly in English engaging external professors and professionals, and often either appear in academic departments with strong application orientations or are induced by requests from the environment, likewise then appearing in application favouring departments, or even in departments of other origins than computer science and mathematics, such as law or business administration.

Master Programmes in Information Security typically extends over one full year, devoting 50-75% of the time to theoretical courses and 50-25% to applied work. Most spring out of research activities and the interdisciplinarity is explained in terms such as 'taught jointly by two departments', ' a curriculum taking a socio-technical approach to the security of information systems', or 'staff comprising members concerned with different relevant areas'.

In all the interdisciplinary oriented programmes and courses there are similarities in structure, extent, duration, level, and more-than-one-subject-orientation, and differences in prerequisites, orientation, and depth. Taken together they cover a wide range of subjects/areas from mathematical/technical, computer science, administrative/managerial/ management and law.

2.3 Origins and effects of interdisciplinary and traditional education

In general interdisciplinary education originates with strong application orientation, while traditional education is established in conjunction with research. There are also traces of commercial versus military origins.

In the area of EDP auditing development of university courses and programmes were conducted jointly by practitioners and academics (Singleton, Flesher and Dale 1994, Kneer, Vyskoc and Gallegos 1994) first for undergraduate levels and later for master and research levels. The result of this policy seems to be that education is strong, while research is weaker (Weber 1994).

Within IT security education the development has been the opposite. Highland (1992) points out that the failure to develop meaningful computer security /education/ is shared by three parties: the academics for being lax in accepting security, the business communities for being unable to specify their own needs, and the military for developing security necessary for their needs but unsuitable for the real world. In parallel, the research area has been fractionalised into at least four specialisations: computer security, cryptography, fault tolerant computing, and software safety (Cohen 1995).The results of these policies taken together seem to be strong research with less focus on education.

This is not surprising; interdisciplinary approaches in general are not favoured by scientific communities, and traditional theoretical approaches are not seen as directly useful by business communities. However, current stated problems include characteristics of both; and that is why we now see the two approaches appearing side by side. The next development step must be to bride these two - from both ends. In order to do this educators must pay more attention to processes of learning and teaching.

3 EDUCATIONAL AND PEDAGOGICAL ASPECTS

In an ideal case there is an available model of the whole area to be taught. This model forms the base for specifying relevant inter- and intra- course structures and contents as well as defining prerequisites and required results in form of knowledge and skills. For choosing suitable pedagogical forms, teaching methods fitting the material, students, teachers, and the educational environment are selected.

In reality there may be some general framework describing the knowledge area used primarily for other purposes than education. Most university courses and programmes seem to have been developed based on general consensus of the area amongst academics and and, to a certain extend, professionals in IT security. And even though there are no references to an explicit framework or model there are mutual understandings about such issues as level, prerequisites, weekly work load, amount of lectures, tutorials and lab work, extension in time, useful scientific theories and methods, etc.

The same is usually true also for non-university based courses and programmes, although most of them are more directly focusing a subarea, a familiar context, or a specific implementation.

However, in order to establish compatibilities and transferabilities between different educational systems, it is useful to have an understanding of the separate educational efforts. I refrain from using the word 'standard' or 'licensed' here, although I strongly believe we need also those procedures for parts of the educational systems or parts of the educations. But let us first investigate some of the existing teaching/learning models within IT security education, because there are not very many. Besides, they often lack or are not easily compatible with pedagogical aspects such as methodologies for disciplinarity and interdisciplinarity, learning and learner oriented teaching, and life long learning.

The most used educational model is merely some kind of framework for specifying the knowledge area. Sometimes this model may also be used to link other official structures, analyse and develop security policies, and audit and evaluate security measures. Only one model has been found addressing specifically security didactic, although general models for active learning also could be applied within our field. In addition, there is a systemic-holistic

model for academic programmes and an /interdisciplinary/ model for incorporating specific issues into computer science programmes.

3.1 Some frameworks and models for specifying the knowledge area

First, in the Joint ACM/IEEE Computing Curricula 1991 (ACM 1991) security was treated as a 'recurring concept', which are those significant ideas, concerns, principles, and processes that can be applied over the total structure and help to unify the academic discipline. The total computer science discipline is specified in nine subject areas which each can be viewed from three paradigms/processes; these are later specified in knowledge units. Recurring concepts such as security may then be used in curricula building as either the focus or as an underlying theme.

Within the European Community, a group of academics in the framework of an Erasmus project, has recently presented a proposal for a one and a half year postgraduate curriculum in Information Security, Dependability, and Safety (Katsikas and Gritzalis 1995). This proposal is not based on an explicit model of the area but rather on research, experiences, common understandings of the area, studies of university courses and programmes (Gritzalis 1995, Yngström 1995b), and knowledge of the varying university regulations. The curriculum is structured on three levels: common mandatory courses, stream mandatory courses and /stream/ elective courses. Suggested streams are Information Systems Security, Dependable Systems and Distributed Systems Security, but other extensions and mixes could be possible. The overall structure is depicted in Figure 1. Each course is further presented with credits, duration, detailed contents description, learning scheme, indicative textbooks and existing similar courses. The continuation of this development will include trimmings of the overall structure to fit into several university environments and developments of varied teaching and learning material.

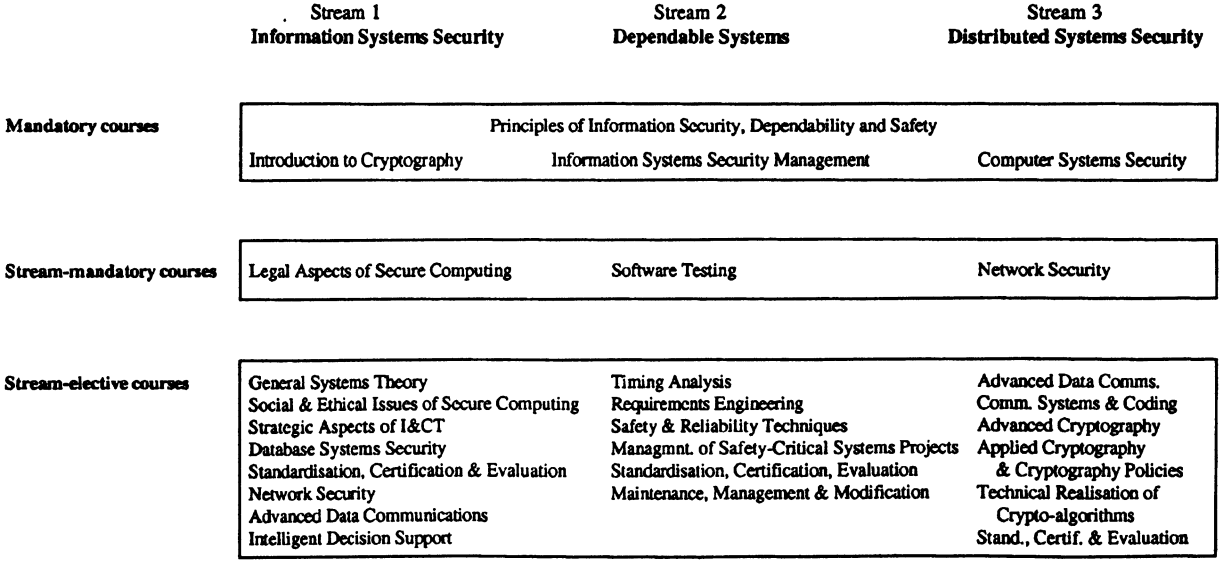

Figure 1 Overall structure of the postgraduate curriculum in Information Security, Dependability, and Safety (reproduced from Katsikas and Gritzalis (1995)).

The GASSP Committee is using the the OECD nine principles of 1992 (OECD 1992) - accountability, awareness, ethics, multidisciplinary, proportionality, integration, timeliness, reassessment, and democracy - as foundations for Generally Accepted System Security Principles. The principles, called Pervasive Principles, are further broken down and defined as Broad Functional Principles, which in turn will be explained through Detailed Principles. Security services and mechanisms will then provide support for the Detailed as well as the Broad Functional Principles. The idea of developing the GASSPs according to Parker (1995) is to have them as well understood and accepted as the equivalent Generally Accepted Accounting Principles are within the accounting world. The GASSP structure will be used as a base for specifying courses and programmes, and is planned to be linked to other accepted security requirements for for instance evaluation and certification purposes.

McCumber (1991) presents a three dimensional model of the area. The first dimension characterises information states into transmission, storage, and processing, the second dimension includes critical aspects: confidentiality, integrity, and availability, and the third dimension includes the security measures technology, policy and practice, education, training and awareness. This model can be used for determining requirements for education, training, and awareness, although he underlines its use for developments, auditing, and evaluation of IT security systems. When used for developments, states of information and their three critical information characteristics are defined, and security measures are chosen as a combination from the three layers of security measures. For auditing and evaluation purposes it may be used similarly: states of information independent of technology are identified, the vulnerability of critical information characteristics are defined, and implemented security measures are evaluated.

The McCumber model has great similarities with the CobiT - Control Objectives for IT - framework (CobiT 1995). CobiT is not an educational framework, but a general and comprehensive structure which can ensure auditors, management, business process owners, and IT security specialists that adequate control systems are provided for the IT environments and thus they can take full responsibilities for all aspects of the business processes. It was developed as a generally applicable and accepted standard for good practices for IT control on the basis of the existing ISACA (the Information Systems Audit and Control Association, former the EDP Audit Association) control objectives, enhanced with existing and emerging technical, professional, regulatory, and industry specific standards. It is aiming to imply the same sense as the 'Generally Accepted Accounting Principles' do and to be applied world-wide to information systems in enterprises.

CobiT offers the possibilities to incorporate - at a lower level - standards, guidelines, codes of conducts, policies, evaluation schemes, security models, etc. It is presently under evolution: Phase one includes defining the framework, linking it to existing control objectives and stating rationales for each control objective. The second phase will consist of specifying audit guidelines, update the automated version and include research material not considered during phase one. The third phase will add control practices, enhance control objectives and identify performance indicators.

The structure is presented as a cube, depicted in Figure 2, with the dimensions IT Processes, IT Resources and Information Criteria. IT Processes are organised into levels Domains, Processes and Activities. IT Resources are categorised as Data, Application Systems, Technology, Facilities or People. Information Criteria, which are the information needs referred to as business requirements, include Quality, Fiduciary and Security; in Quality are

included Quality, Cost, and Delivery, in Fiduciary Effectiveness and efficiency of operations, Reliability of financial reporting, and Compliance with laws and regulations, and in Security Confidentiality, Integrity and Availability.

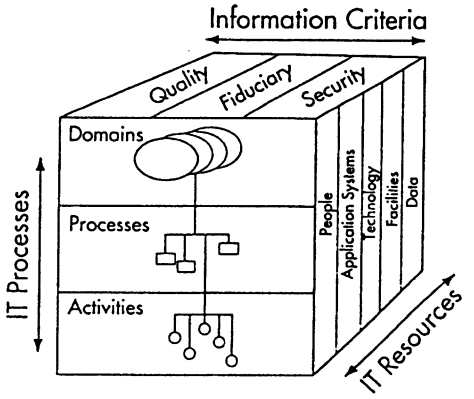

Figure 2 The CobiT framework (reproduced from CobiT (1995)).

The framework may be approached from either one of the dimensions. To facilitate efficient use of the control objectives, navigation aids are provided as part of the presentation of the high level IT control objectives. This way it is possible to know where in the structure and with which aspects a specific fact is treated.

3.2 Models for incorporating pedagogical and methodological aspects

Within general engineering education Kolb's cyclic model of learning has been used for developing students' abilities to enhance theoretical knowledge with practical experiences (Kolb 1984, Smith 1991). The model includes four main processes: Reflection includes individual gathering of information, Conceptualisation includes group discussions, laboratory work, interpretations and critical thinking, Planning includes hypothesis formulation, group experiments to improve certain parts, and planning for implementations, and Implementation includes individual laboratory work, reviewing, hypothesising, and presenting. Within and between each main process there are feed-back loops for refining and enhancing individual learning.

In a framework, based on a psycho neuronal model of learning, Machonachy (1989) presents a structure with the goal to internalise the notion of security into each student. The framework, seen in Figure 3, is a learning continuum consisting of three levels: awareness,

training, and education. Each program, module, and session of the education has to cover and remind the student of this continuum and the model is exemplified by activities for each level.

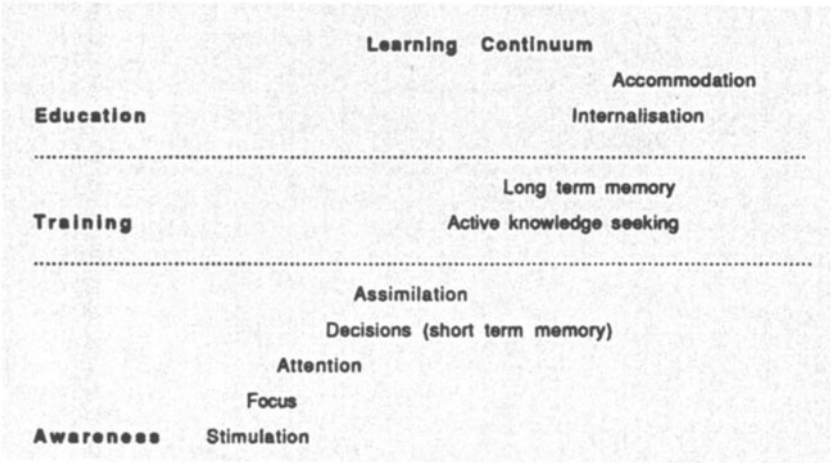

Figure 3 Machonacy's model of a learning continuum (after Machonachy(1989)).

Awareness needs stimulation, focus, attention, decisions, and assimilation. Training involves actively seeking more knowledge and using the long term memory, while education involves internalisation and accommodation of the content learnt.

Stimulation wakes up the learner, focus makes her delimit the problem from its environment, attention reinforces the problem, decision makes her intentionally remember the problem, and assimilation makes her understand the whole problem.

Training makes the learner active in seeking and remembering knowledge for specific skills, whereas education facilitates the learning to internalise and accommodate fundamental and generalised principles.

The systemic-holistic approach developed and used for programmes and courses on undergraduate and master levels, as presented by Yngström (1994, 1995a), uses two parts: one three dimensional framework describing the contents, the level of abstraction, and the context, and one systemic module which acts as an epistemology for control. Together the framework and the module specifies the areas of control as well as the theories, and general and specific methods of control. The conceptual model for the programme is presented in Figure 4.

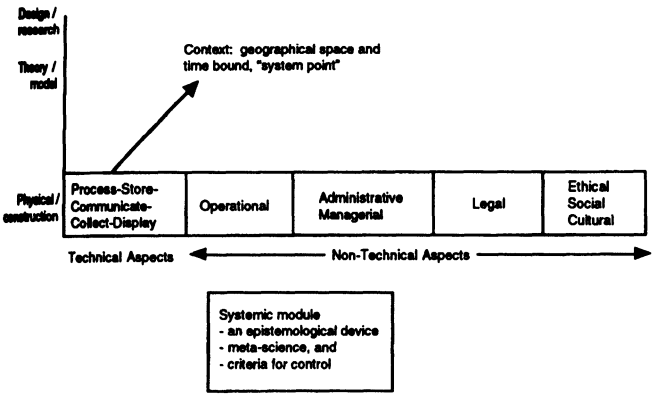

Figure 4 The conceptual model for IT Security education based on the systemic-holistic approach (reproduced from Yngström (1995)).

This model was originally developed for educational purposes from criteria derived from extensive analyses of state-of-the-art in IT security. Criteria concern: support a systemic-holistic approach as well as studies of physical and symbolical levels - in and out of context, include all fundamental questions and significant accomplishments, be open and flexible to incorporate changes and new possibilities and yet delimitable, be recursively applicable on identified levels, support generalised, specialised, intradisciplinary and interdisciplinary studies, be realisable in different academic environments, on different levels and under different circumstances, and support life-long learning. Reported evaluations (Yngström 1995a, 1993) support positively the systemic-holistic approach as facilitating assessment and understanding of problems, increase work efficiency and effectiveness and foster continuous learning.

The ImpactCS Project (1995) presents a structure for interdisciplinary courses, most particularly how to incorporate teaching and learning about social and ethical impacts of computing into a computer science curricula. A structure based on levels of Social analysis and topics of Ethical analysis is integrated with different technologies, such as electronic communication and medical technology to form a conceptual three dimensional framework. Each intersection in the framework has the possibility of forming a study unit in which a particular level of Social analysis, Topic of ethical analysis and a physical implementation is studied. There are many different ways to study these questions, however student centred learning is favoured over lectures. The project will in the next phase give examples of such units including supporting material and methods.

3.3 New directions needed

It is quite clear to me, owing to quests for interdisciplinary approaches, for taking account of political, cultural, social, commercial, and technical needs, for intensifying efforts of

awareness, and for overcoming the fractionalised research that the time has come to balance our education in favour of more student centred activities. "Learning by doing" is an old device - and can be used for interdisciplinary as well as for disciplinary education. The younger generations have, as Highland (1992) points out, grown up with Sesame Street and computer games, and it is high time to bring some edutainment into our programmes and courses. Good and valuable education must not be difficult and boring, on the contrary, every teacher knows that learners with keen interests and curiosity usually learns even difficult material better and quicker than uninspired students. MACIS were the acronyms we were taught in teacher's training college: M for motivation, A for activity, C for concrete, I for individual and S for synthesis. Those are the main tasks of a teacher, besides knowing her subject.

Moreover, the Information Society era will change people's understanding of the needs for security through their own experiences. In some European countries there are now movements for introducing a general computer drivers license, which also offers opportunities to incorporate necessary knowledge and skills in IT security for the citizens. And then again, I predict the privacy issue will be a very good vehicle for understanding the needs of balanced efforts within IT security.

In between the regular citizen and the university educated IT security professional, there are large groups of professionals and members of various workforces who all will need more knowledge, understanding, and skills. They will, as the rest of the population, also need learning centred education following MACIS.

4. REFERENCES

ACM (1991) *Computing Curricula 1991. Report of the ACM/IEEE-CS Joint Curriculum Task Force*, ACM Press & IEEE Computer Society Press.

Burns, A., McDermid, J. and Dobson, J. (1992) On the Meaning o Safety and Security., in *The Computer Journal* **35:1**, 3-15.

CobiT (1995) *Control Objectives for Information Technology. CobiT Framework*, Exposure Draft, August 1995, CobiT Steering Committee; the Information Systems Audit and Control Foundation Research Board and the Information Systems Audit and Control Foundation Standards Board.

Cohen, F.B. (1995) Viruses, Corruption, Denial, Disruption, and Information Assurance, in *Information Security - the Next Decade* (eds. Jan H.P. Eloff and Sebastian H. von Solms), Chapman & Hall, London.

Gritzalis, D (ed.) (1995) *University Programmes on Information Security, Dependability and Safety*, European Commission, Erasmus ICP Project ICP-94(&95)-G-4016/11, Report IS-CD-3c, Athens.

Higgins, John C. Information Security as a topic in undergraduate education of computer science, in *Proceedings from the 12:th National Computer Security Conference*, 1989.

Highland, H.J. (1992) Perspectives in Information Technology Security, in *Education and Society Information Processing 92*, Volume II (ed. R.M. Aiken), IFIP Transactions A-13, North-Holland, Amsterdam.

ImpactCS (1995) *Consequences of Computing: A Framework for Teaching the Social and Ethical Impact of Computing* . A Report from the ImpactCS Steering Committee, May, 1995, George Washington University, Washington.

INFOSEC (1992) *Information Security INFOSEC'92. Security Investigations,* European Commission DGXIII/F-GE1190/GI, reviewed, 22nd Jan 1992, Brussels.

Katsikas, S. and Gritzalis, D. (eds.) (1995) *A proposal for a postgraduate curricula on information security, dependability, and safety*, European Commission, Erasmus ICP-94(&95)-G-4016/11, Report IS-CD-4a, Athens.

Kneer, Dan, Vyskoc, J., Gallegos, F. (1994) Information Systems Audit Education, in *IS Audit & Control Journal,* **Vol IV**, 13-20.

Kolb, D. (1984) *The cyclic model of leaning*, Prentice Hall, N.J.

Lévy-Strauss, Claude (1968) *The Savage Mind*, University of Chicago Press, Chicago.

Lunheim, Rolf and Sindre, Guttorm (1994) Privacy and computing: a cultural perspective, in *Security and Control of Information Technology in Society* (eds. R. Sizer, L. Yngström, H. Kaspersen, S. Fischer-Hübner), IFIP Transactions A-43, North-Holland, Amsterdam.

Maconachy, W. (1989) Computer Security Education, Training, and Awareness: Turning a philosophical orientation into practical reality, in *Proceedings from the 12th National Computer Security Conference*, Baltimore.

Martin, C.D. and Holz, H.J. (1992) Integrating Social Impact and Ethical Issues Across the Computer Science Curriculum, in *Education and Society Information Processing 92*, Vol II (ed. R.M.Aiken), IFIP Transactions A-13, North-Holland, Amsterdam.

McCumber, J. (1991) Information Systems Security: a Comprehensive Model, in *Proceedings from the 14th National Computer Security Conference*, Washington.

Miller, K. (1988) Computer Ethics in the Curriculum, in *Computer Science Education*, **1**, 37-52.

National Research Council (1991) *Computers at Risk. Safe Computing In the Information Age*, Systems Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press.

OECD (1992) *Guidelines for the Security of Information Systems,* Organisation for Economic Co-operation and Development, OECD/GD(92)190, Paris.

Parker, D. interview (1995) Computer Security as Folk Art: Why We Need the GASSP, in *Computer Security Journal*, **Vol. X, Number 2**, 1-4.

RDF, Riksdataforbundet (1986) *En Svensk tiger - introduktion till ADB-sakerhet och sarbarhet.* Skogs Reklamlito, Malmo.

Siklossi, K (1966) *Cybernetic teaching*, Prentice Hall, N.J.

Singleton, T., Flesher, Dale.L.(1994) The Developments of EDP Auditing Education, Research and Literature in North America: 1977 to 1994, in *IS Audit & Control Journal*, **Vol. IV**, 51-60.

Smith, R.A. (1991) *Innovative teaching in engineering*, Ellis Horwood, Chichester.

Turkle, Sherry (1990) Style as Substance in Educational Computing, in *The Information Society: Evolving Landscapes* (eds. J. Berleur, A. Clement, R. Sizer, D. Whitehouse), Springer-Verlag, New York.

Weber, R. (1994) The Evolution of the EDP Auditing Interviews, in *IS Audit & Control Journal*, **Vol. III**, 2-3.

Yngström, L. (1993) Evaluation of an academic programme in IT Security 1985-1990, in *Computer Security: Discovering Tomorrow* (eds. Graham E. Dougall and Darren Jones), North-Holland, Amsterdam.

Yngström, L. (1994) Education in IT Security at Bachelor and Master Levels Using a Systemic-Holistic Approach, in *Security and Control of Information Technology in Society* (eds. R Seizer, L. Yngström, H Kaspersen, S. Fischer-Hübner), IFIP Transactions A-43, North-Holland, Amsterdam

Yngström, L. (1995) A Holistic Approach to IT Security, in *Information Security - the Next Decade* (eds. Jan H.P. Eloff and Sebastian H. von Solms), Chapman & Hall, London.

Yngström, L. (1995b) Education in IT security in Europe, in *IFIP/TC11/WG11.8 workshop "Current and Future Needs, Problems and Prospects"* May 8, Capetown, South Africa. (can be obtained through the author).

7 BIOGRAPHY

Louise Yngström is an ass professor at the department of Computer and Systems Sciences at Stockholm University and Royal Institute of Technology. She has been with the department since 1968, engaged in research and education in Information Retrieval Systems, Computer Aided Instruction and now since 1985 in Security Informatics. She started IT security education based on systemic principles, which she wrote her licentiate thesis on in 1992. Presently she is finalising her PhD on the systemic-holistic approach to IT Security education. She is chairperson of TC11/WG11.8 "Infosec education", Swedish representative to TC11, and member of IFIP workinggroups TC9/WG9.2 and 9.6. She is devoted to a humane Information Society and is a mother of four.