Full-Spectrum Information Security Education: Integrating B.Sc., M.Sc., and Ph.D. Programs

Erik Hjelmås
Gjøvik University College
NISlab, Dept. of Computer Science and Media Technology
P.O. Box 191
2802 Gjøvik, Norway
erikh@hig.no

Stephen D. Wolthusen
Gjøvik University College
NISlab, Dept. of Computer Science and Media Technology
P.O. Box 191
2802 Gjøvik, Norway
stephenw@hig.no

ABSTRACT

In this paper, we describe the content and rationale of a comprehensive information security program encompassing degree options at the B.Sc., M.Sc., and Ph.D. levels established at Gjøvik University College, Norway. While the individual programs are open for students meeting certain formal prerequisites at each level, the sequence of degree programs is also designed in such a way as to allow students to progress from B.Sc. to Ph.D. levels without undue overlap or repetition.

This is accomplished by placing different emphases on the teaching and learning tools and techniques used, moving on to higher levels in Bloom's hierarchy in the process. At the same time, the different degrees also take into account the career progression and concomitant changes in the needs of students. We describe these considerations along with a brief description of courses offered at each level, along with a description of the learning environments at each level.

Categories and Subject Descriptors

K.3.2 [**Computing Milieux**]: Computer and Information Science Education—*Curriculum*

General Terms

Security

Keywords

curriculum development, information security

1. INTRODUCTION

The education of information security professionals is a growing activity in many universities and colleges worldwide. At Gjøvik University College, Norway, a dedicated two-year Master of Science in Information Security program was initiated in 2002, with a Bachelor of Science in Information Security having been added in 2005 owing to considerable interest from industry. In addition, a doctoral program in information security is being established and preparing for independent accreditation. A first cohort of Ph.D. students entered this program in 2003. All research and teaching activities in the research group dedicated to information security are focused in the Norwegian Information Security Laboratory (NISlab), which provides a research-intensive environment in which students at all levels can collaborate and be guided by faculty members and postdoctoral research staff. Considerable attention has thus far been devoted to information security (or information assurance) education over the past decade with conference series such as CISSE [6], WECS [5], WISE [10], and InfoSecCD [16][13] devoted to the subject and a vibrant community [8]. Most research in this field, however, has been devoted to individual strands of a full information security education curriculum such as undergraduate programs. In this paper we therefore discuss issues and opportunities arising from providing a full spectrum information security program with degrees offered at the B.Sc., M.Sc., and Ph.D. levels at the same time. Of particular interest in this context is the development of a progression of core information security courses which, while offering immediate entry points for students from core disciplines such as mathematics, computer science, or electrical engineering at each level, nevertheless provides new and challenging knowledge and insights for students progressing from information security degrees. Another key aspect requiring careful consideration in the design of the curriculum is the career progression of students and the changing composition of the student body at higher degree levels. Here, not just the content of the curriculum but also its delivery and the objective for fostering learning as the focus increasingly requires shifts to analytical and synthetic learning [3][1]. In this paper we describe the ongoing process at NISlab for providing such an integrated curriculum and curriculum development at the B.Sc., M.Sc., and Ph.D. levels in which research in the rapidly developing sub fields of information security informs the curriculum development at the same time that external factors such as student requirements and needs as well as the differing requirements for careers in industry, academia, and government are taken into account.

The remainder of this paper is structured as follows: Section 2 briefly reviews related programs at both the undergraduate and also graduate levels with an emphasis on degree programs with explicit specialization in information security. In section 3, we describe the interrelationship between the degree programs and the anticipated requirements as students progress in their careers, irrespective of whether this career is to take place in industry or academia while sections 4 and 5 describe the impact of the requirement to take both direct academic progression to the M.Sc.

Information Security Curriculum Development (InfoSecCD) Conference'06, September 22-23, 2006, Kennesaw, GA, USA.

and Ph.D. levels as well as mid-career professionals into account. Section 6 then provides an overview of the current core course offerings at each of the academic levels, and section 7 offers our current outlook on the continued development of these programs.

2. ACADEMIC LEVELS

As described briefly in section 1, there exist several conference series addressing information security education with a considerable portion of the papers at these conferences devoted to various aspects of curricular development. Given the origins of most information security programs, much of this earlier work initially focused on various aspects of adding and integrating information security into existing curricula [12]. However, as colleges and universities are increasingly beginning to offer dedicated programs in information security and also broaden the scope of these programs beyond undergraduate studies, this is also beginning to be reflected in the relevant literature [9]. One of the earliest such graduate programs was developed at Royal Holloway, University of London, UK (RHUL) where a M.Sc. program in information security has been established in 1992, making this one of the very first such programs worldwide [4]. The program is focused more towards professional than academic careers, and contains four core modules: "Security Management", "Introduction to Cryptography and Security Mechanisms", "Network Security" and "Computer Security", accompanied by several elective modules and a M.Sc. project. This general outline of the curriculum at the M.Sc. level in the form of the core courses appears to be widely recognized and replicated in M.Sc. programs established elsewhere following in the image of the RHUL program, although the relative emphasis on cryptographic topics varies somewhat. As noted above, the RHUL program admits students with both technical and management backgrounds into the information security program while a second M.Sc. degree program in the Mathematics of Cryptography and Communications established in 2005 is devoted solely to cryptography. Even though the earliest efforts at information security academic programs were at the graduate level with specialized course offerings typically dictated by faculty research interests, considerable attention has since been devoted to the systematic curricula design process of academic programs particularly at the undergraduate level.

Much of this effort was concentrated in the program for "National Center of Academic Excellence in Information Assurance Education" established by the U.S. National Security Agency in the form of the National Information Assurance Education & Training Program (NIETP), which also sponsors the CISSE conferences series. In this program, East Stroudsburg University of Pennsylvania was the first institution to award a B.Sc. in computer security [11]. This program encompasses six core modules: The courses "Fundamentals of Security Engineering", "Risk Analysis / Certification and Accreditation", "Applied Computer Cryptography", "Legal Impacts of Computer Security Solutions", "Applied Network Security", and a module "Security Engineering Internship". Much of the same course topics are also present in the undergraduate information assurance program at ITOC, United States Military Academy, West Point as described in Conti et al. [7] and in other CoE accredited undergraduate programs in the U.S. However, Conti et al. also describes to importance of information security integration throughout the curriculum, which cannot be constrained solely to specialized courses. There are several other e□orts at developing undergraduate programs as well, the most notable probably being Whitman and Mattord at Kennesaw State University [15]. The efforts of Whitman and Mattord has resulted in a model curriculum for information assurance and security and provides a comprehensive approach for a B.Sc. degree program that is complementary to the CoE approach; this document also contains proposed syllabi for the entire program [14].

Beyond the above mentioned programs, however, information security is typically taught as a concentration within an existing program at the graduate level; given this constellation, the authors are not aware of literature addressing the explicit progression within the field from the B.Sc. onward to M.Sc. and Ph.D. programs, particularly with students from diverse backgrounds and educational pathways entering the programs both in mid-stream and progressing linearly through each program. However, a general outlook on the different goals of education in information security undergraduate, M.Sc., and doctoral level is described by Bishop [2], although the issue of heterogeneous entry of student populations at the graduate level is not explicitly addressed.

3. CAREER PROGRESSION

The qualification profiles for information security graduates at the different levels can be distinguished quite clearly and also represents a career progression model, particularly for students which return for a M.Sc. or Ph.D. after gaining work experience. Graduates at the B.Sc. level, even if the degree in information security is a second degree, may be expected to fill primarily entry-level positions in the information security field. At this level, positions are typically closely integrated into IT operations, and the distinction between system and network administration in general and security-specific knowledge and skills is not yet fully formed. Graduates at the B.Sc. level must therefore possess a solid background not only in information security but also in the ancillary network and operating system areas which enable a clear understanding of requirements, processes, and operations. This additional background also provides important synoptic skills for the analysis of complex problems and configurations and the interactions between various components which may be pertinent to security issues.

Key to this systems-level understanding is the development of mental models on the part of students of the relevant components and networks; this can only partially be accomplished through the acquisition of declarative knowledge. Rather, it is also necessary to gain a certain amount of operational knowledge as only the combination of both types of learning enables the integration of knowledge to the point where students acquire the heuristics and skills necessary for addressing security problems in complex systems. At the M.Sc. and, with some modifications also at the Ph.D. level, this concentration on operational aspects and issues is no longer the foremost qualification required. While a solid grounding in an operational background and of supporting areas such as networks, operating systems, and cryptography is still of utmost importance, the key distinction beginning with the M.Sc. degree program is the increased requirement to formulate problems and models at higher levels of abstraction and sophistication. This reflects the more strategic or architectural orientation expected of senior or mid-career information security

specialists. The emphasis in both coursework and individual tutoring therefore also shifts to a more abstract and theoretical framework on which students are expected to build their own research and knowledge profile. At this level, moreover, it is to be expected that an increased differentiation into career profiles and specializations takes place, which is not necessarily desirable at the B.Sc. level where a more generalist foundational knowledge must be built up.

To this end, elective coursework, term papers, and individual studies is designed to enable students to concentrate on the major career pathways for mid- to senior-level information security specialists. The main areas we identified in this context are security architectures and operational security, security in software engineering and system integration, and digital forensics. In each of these cases, the focus is on providing the information security-specific aspects of knowledge and foundations for further research and investigation. However, it is obvious that a significant portion of the body of domain knowledge pertinent for each of the specialization areas must be acquired separately by the students. For several of the pathways noted above, there are also clear requirements for knowledge of the legal issues surrounding the field. This is at least somewhat problematic in that students entering into the information security programs at all levels are typically not acquainted with the concepts and mental models of the legal profession. Taught courses can, in this context, only provide a rudimentary overview of the issues at hand and the requirement for consultation and coordination with the relevant experts. This is particularly the case since even at the level of small and medium enterprises or government offices, it is frequently the case that one is not only confronted with ones own national legal framework and models of jurisprudence but, moreover, also has to take into account cross-border and international legal concerns. A final core element that is of particular importance to the operational and forensics career pathways is the inclusion of not only legal aspects and considerations but also of ethical issues frequently arising in the discharge of duties of information security professionals. The anticipated differences in career profiles in the fields previously described between the M.Sc. and Ph.D. levels are of a more quantitative nature and less pronounced than between the B.Sc. and M.Sc. levels; however, the additional pathway of preparing doctoral students for academic research and teaching must be taken into consideration.

Particularly the latter pathway requires a broader exposure of Ph.D. students to research design and methodology beyond the immediate requirements of a student's thesis and preparing for possible postdoctoral work or subsequent supervision of research. This is an area that is frequently emphasized insufficiently in engineering and computer science environments and can often result in avoidable errors and weaknesses. A further key aspect of preparing doctoral students in information security for independent or minimally guided research is the consideration of research ethics and codes of conduct. Particularly in cases where research includes the derivation of empirical results and involves end users, students must have a firm grasp of both legal and ethical constraints on such research, e.g. by considering privacy issues prominently in the design of studies and analyzes. One aspect which can be supported and encouraged in Ph.D. and M.Sc. students, but not be formed in full by the program is the development of a certain mathematical maturity on the part of students; depending on the area of specialization for research a student may wish to pursue, this can encompass the acquisition of specialized techniques and knowledge; the core emphasis, however, must be on skills such as problem solving, proof, and, analytical skills. Another challenge which cannot be fully met by formal education processes is the maturation and acquisition of experience and skills that arise from practicing in the field and interactions in a working environment. In this area, mature and returning students enjoy an advantage which can only be partially compensated through encouraging group learning and laboratory time.

4. INHOMOGENEITY OF LEARNING EXPERIENCES

Disregarding the possibility of students enrolling for a second undergraduate degree, the career progression model described in section 3 also has a direct impact on the characteristics of the courses and materials which can be taught at the B.Sc. and M.Sc. levels.

Students entering into the undergraduate program from secondary education are both largely homogeneous in their background and most comfortable with taught courses which closely resemble their learning experiences thus far. A key objective during the course of the program is therefore to encourage students to broaden their learning skill set by conducting independent research, including primary literature sources as well as group-based activities such as programming and security administration projects. These skills are critical both to subsequent academic progress largely independent of the subject area pursued and also for continued learning in a professional context. In particular, the ability to locate and critically analyze complex academic and technical information is vital for maintaining currency in a rapidly advancing field, yet the necessary learning tactics differ markedly from those required for the absorption of the concise and condensed information typically found in textbooks.

The considerable heterogeneity of students entering into the M.Sc. program extends not only to the academic and technical background but also to the learning techniques and strategies which the students have acquired. These will differ markedly particularly for students entering the program directly from an undergraduate program (regardless of whether this is the B.Sc. in information security or another program) and mid-career professionals that are released, often on a part-time basis, by their employers or are re-training. While students in the latter category may experience difficulties with foundational material requiring mathematical and computer science skills they have not exercised for an extended period and consequently will have to re-learn at least in part, this is more than balanced by the problem-solving skills and heuristics they have acquired in their professional experience. These also benefit other students directly progressing to the M.Sc. program during joint work and project assignments. Moreover, this diversity within the program also provides an additional benefit during taught courses in that the perspectives of mature students allows them to relate material which appears abstract at first to real-world experiences and therefore to emphasize the relevance of the taught material not only for themselves but also indirectly for other students, which stand to gain additional motivation not just regarding the taught material but also for further investigation.

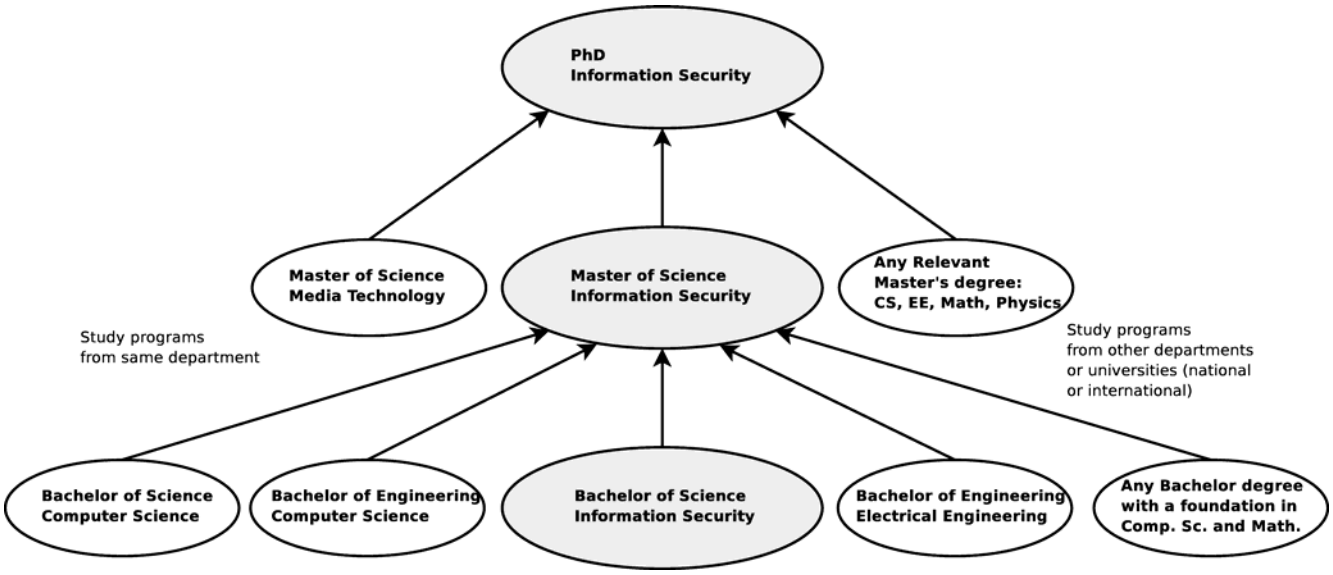

Figure 1: An overview of possible pathways leading to an information security program at Gjøvik University College.

5. DELIVERY CONSIDERATIONS

Several factors must be taken into consideration for the delivery of taught material for the M.Sc. program. As is typical for other programs worldwide, mature students, particularly on release for the program, are typically taking the courses in the program over an extended period and, moreover, may not be able to physically attend all course sessions. At the same time, given that the program in Gjøvik is a national magnet program, students may also not be living on or near the college campus but rather commute to the college for classes and other activities. This has several important implications. First, it is highly desirable to concentrate courses into consecutive days to ensure that students' travel and other preparation time is minimized. This is also of benefit to resident students as it allows them greater flexibility. By providing audiovisual recordings as well as live streaming with the possibility of remote interaction, further opportunities for the delivery of course material are provided, particularly for situations when it may not be possible for students to be present at the campus for a given lecture.

The second implication, however, is that taking part-time attendance into account limits flexibility in adjusting the timetable of the program as students may expect to take courses in a certain pre-determined sequence. Beyond reordering of course offerings, another restriction of a sizable part-time student population is that course offerings (e.g. elective modules) cannot realistically be changed within a single iteration but should be phased out to allow part-time students to take such courses. However, given the speed of development in some research areas at the graduate level, it is nevertheless necessary to update course offerings to reflect current research so that students taking a year longer to complete the program will in some cases be dealing with different (typically more advanced and more recent) material from their peers.

6. STRUCTURE OF THE PROGRAMS

Norway has adopted the European "Bologna system" aimed at harmonizing higher education across Europe and encouraging mobility and credit transfers with three-year B.Sc., two-year M.Sc. and three-year Ph.D. programs (where one year equals 60 credits in the European Credit Point Transfer System (ECTS) and approx 1500-1800 working hours for a student). It should be noted that a three year bachelor program means that the program is focused and "narrow" already from the first semester with courses solely in the subject area and its prerequisites but omitting general education and other subjects. Figure 1 shows different paths students may follow when pursuing an information security education at Gjøvik University College. At Gjøvik, a semester system is in operation with the fall semester stretching from August until December, and a spring semester from January until June. The course codes represent the course level with the first digit indicating the typical year of study at the B.Sc. level, i.e. 1000 to 3000 series courses in the B.Sc. program, 4000 and 5000 series courses are M.Sc. courses, and 6000 series courses encoding Ph.D. research seminars or advanced topics.

6.1 B.Sc. Course Structure

The B.Sc. in information security is closely tied with the computer science program and follows the same core courses (programming, algorithms, operating systems, databases, software engineering, etc). Out of 180 ECTS credit points, only 60 points are specific to the information security program. The courses developed for the B.Sc. are:

6.1.1 Introduction to Information Security

This is a 10 credit course in the first year (1000-level) running in the first (fall) semester serving to introduce the students to concepts and motivate them for the program. Upon completion of this course the students will have acquired knowledge of concepts and topics within information security. The students will also know about the national laws and regulations applying to the field

of information security, with special emphasis on the laws regulating personal information. Furthermore, the students will know about relevant national and international norms and standards within information security.

6.1.2 Introduction to Security Management

This is a 10 credit course also in the first year (1000level) running in the second (spring) semester where the students do much hands-on work in security management. Upon completion of this course the students will be able to perform a risk analysis by means of a ROS-analysis, and to perform information security work according to the standards studied.

6.1.3 Data Communication and Network Security

This is a 10 credit course in the second year (2000-level) running in the fourth (spring) semester where the students are introduced to computer networks with a particular emphasis on security aspects in networks. Upon completion of the course, the students will understand the most commonly used standards and protocols for data communication and the principles of network security.

6.1.4 System Administration

This is a 10 credit course in the third year (3000-level) running in the fifth (fall) semester intended to provide students with the important practical experience of setting up a network and computing infrastructure. Upon completion of the course, the students will be able to administrate users, computers, networks and software, plan and implement a simple, stable and scalable infrastructure. The students will also master the basic requirements of security in such an infrastructure.

6.1.5 Security in Operating Systems, Databases and Software

This is a 10 credit course in the third year (3000-level) running in the fifth (fall) semester, and is a classical computer security course. Upon completion of the course, the students should understand the security mechanisms of operating systems and databases, understand the general problems in software security and be familiar with the most common software vulnerabilities.

6.1.6 Cryptology

This is an optional (but mandatory in the M.Sc. program) 10 credit course in the third year (3000-level) running in the fifth (fall) semester where students are introduced to the mathematics and applications of cryptology. Upon completion of the course, the students should be familiar with the mathematical fundament needed to understand the most commonly used cryptographic algorithms, and understand how cryptology is used to achieve confidentiality, integrity, non-repudiation and authentication, the application of cryptographic algorithms and their limitations, and how an encryption algorithm can be designed and analyzed.

6.1.7 B.Sc. Project

All students in the final semester (spring, third year) have to spend 20 ECTS credit points (500-600 working hours) working on a project. The general learning objectives of the project is to learn how to execute a larger independent task of interdisciplinary nature, plan, find solutions and produce documentation of these, getting comprehension of advantages and drawbacks of working in a group, realize the importance of making and following up structured plans, getting a positive attitude to method and problem-oriented way of work and an ability to assess different alternatives.

6.2 M.Sc. Course Structure

Among 120 ECTS credit points required for a M.Sc. degree, we allow 20 credits to be B.Sc. courses to allow for some overlap with the B.Sc. course structure. 10 of these credits are the Cryptology course which is identical for the B.Sc. and M.Sc. level (but only mandatory for the M.Sc. level). Students coming from the B.Sc. Information Security program are required to substitute the Cryptology course in the M.Sc. program with an alternate elective course (e.g. an advanced cryptography course or seminar); there is no credit transfer possible between the programs.

6.2.1 Security Management

This is a 10 credit course in the first year (4000-level) running in the first (fall) semester giving the students insights into the role and responsibility of a security manager. Upon completion of the course, the students should fully understand the complete information security value-chain, fully understand the importance of and challenges and possibilities regarding management focus on information security, be able to create, maintain and develop a security culture based on good attitudes, necessary security awareness and motivation among the employees. The students should also be able to establish and run a suitable and business related security management organization, enjoy the knowledge to master essential standards, frameworks, principles and methods regarding risk management and risk analysis, and have a thorough understanding of system analysis methods applied to information security.

6.2.2 Information Security and Security Architecture

This is a 10 credit course in the first year (4000-level) running in the first (fall) semester and is the graduate level computer security course. Upon completion of the course, the students should fully understand the common terminology and security models in information security, the security mechanisms of operating systems and databases, the general problems in software security and the problems of randomness.

6.2.3 Network Security

This is a 10 credit course in the first year (4000-level) running in the second (spring) semester building on the cryptology course with the applications of crypto in computer networks. Upon completion of the course, the students should fully understand the fundamental problems in network security, the security services and protocols to ensure confidentiality, integrity, availability, authentication, and non-repudiation, and master the use of typical security software for network communication.

6.2.4 Information Society and Security

This is a 5 credit course in the first year (4000-level) running in the second (spring) semester providing the students with insight into the vulnerable infrastructure of our society. Upon completion of the course, the students shall primarily understand the evolution that has taken place within ICT during the last ten years that has led us toward a vulnerable society, and what vulnerability

means in such a broad context. The students shall get suffcient insight to identify, evaluate and implement countermeasures that can protect businesses and organizations.

6.2.5 Legal Aspects of Information Security

This is a 10 credit course in the first year (4000-level) running in the second (spring) semester introducing the students to the some of the many legal aspects of information security they might encounter. Upon completion of the course, the students should be able to account for information security issues within the data protection law, administrative law, criminal law, law on digital signatures, national security law, and banking and finance law.

6.2.6 Scientific Methodology

This is a 5 credit course in the first year (4000-level) running in the second (spring) semester introducing the students to the main issues in scientific thinking. Upon completion of the course, the students should fully understand the main concepts in using scientific methodology, including hypotheses testing and design of experimental studies.

6.2.7 Security Metrics

This is an optional 5 credit course in the second year (5000-level) running in the third (fall) semester giving the students overview of ways to measure security. Upon completion of the course, the students should master how to formulate and measure security related requirements, what degrees of security/compliance are conceivable, and how can compliance be documented.

6.2.8 Payment Systems and Non-repudiation

This is an optional 5 credit course in the second year (5000-level) running in the third (fall) semester providing the students with an overview of electronic payment systems. Upon completion of the course, the students should fully understand payment systems: electronic checks, credit cards, electronic bills and electronic coins, blind signature and anonymity, the principles of non-repudiation.

6.2.9 Research Design

This is a 10 credit course in the second year (5000-level) running in the third (fall) semester giving the students the ability to do practical research design. Upon completion of the course, the students should master how to frame research problems and questions, to develop a plan for conducting a scientific project and to report the results from scientific projects. It is desirable, though not mandatory, that this research plan is immediately applicable to the M.Sc. thesis described in the following section.

6.2.10 Master Thesis

In the spring semester of the second year, the students spend all their time (30 credits) performing research (often with an external industry or research partner involved in the formulation of the research problems and in some cases also in the supervision and guidance of students) in a master thesis.

6.3 Courses for both B.Sc. and M.Sc.

We have also developed a set of elective courses which exist in versions for both B.Sc. (3000) and M.Sc. level (4000). This is accomplished by some differentiation in the included material but also by separating learning objectives within Bloom's taxonomy. In practice this results in the contents of the coursework consisting largely of the same lectures, but with differentiation occurring in exams and additional scientific requirements (e.g. reading assignments) for M.Sc. students in the 4000 series.

6.3.1 Information Warfare

This is an optional 5 credit course running in the first half of the fall semester. Upon completion of the 3000-version of this course, the students should comprehend the concepts of of information warfare: computer crime, cybercrime, corporate espionage, and information terrorism. Upon completion of the 4000-version of this course, the students should fully understand information warfare concepts of computer crime, cybercrime, corporate espionage, and information terrorism, and be able to identify and apply countermeasures.

6.3.2 Authentication

This is an optional 5 credit course running in the first half of the fall semester. Upon completion of the 3000-version of this course, the students should comprehend different authentication methods for example passwords/PIN, fingerprint, facial recognition, iris, tokens, and how authentication methods can be tested. Upon completion of the 4000-version of this course, the students should fully understand different authentication methods for example passwords/PIN, fingerprint, facial recognition, iris, tokens, and how authentication methods can be tested. This difference from the survey character of the 3000 series approach is typically manifested in term paper assignments for studying specific sub-problems at greater depth and students having to independently research the primary and, in some cases, secondary literature.

6.3.3 Perimeter Security

This is an optional 5 credit course running in the first half of the fall semester. Upon completion of the 3000-version of this course, the students should comprehend firewalls and IDS in perimeter security context and how to design a network security policy. Upon completion of the 4000-version of this course, the students should fully understand firewalls and IDS in perimeter security context and how to design a network security policy. Differentiation in this and in the subsequently described courses is as described above.

6.3.4 Intrusion Detection and Prevention

This is an optional 5 credit course running in the first half of the fall semester. Upon completion of the 3000-version of this course, the students should comprehend the mathematical fundament needed to understand intrusion detection and prevention, and applications of misuse based an anomaly based IDS and their limitations. Upon completion of the 4000-version of this course, the students should fully understand the mathematical fundament needed to understand intrusion detection and prevention, applications of misuse based an anomaly based IDS and their limitations, and how an IDS/IPS quality can be assessed and an ability to carry out the assessing process.

6.3.5 *Wireless Communication Security*

This is an optional 5 credit course running in the first half of the fall semester. Upon completion of the 3000-version of this course, the students should comprehend basic concept of wireless communication technology, wireless communication security threats and secure communication protocols. Upon completion of the 4000-version of this course, the students should fully understand basic concept of wireless communication technology, wireless communication security threats and secure communication protocols.

6.3.6 *Incident Response and Computer Forensics*

This is an optional 5 credit course running in the first half of the fall semester. Upon completion of the 3000-version of this course, the students should comprehend the basic principals, methods and tools used in computer forensics and incident response and how to create policies and procedures for computer forensics and incident response. Upon completion of the 4000-version of this course, the students should fully understand the basic principals, methods and tools used in computer forensics and incident response, how to create policies and procedures for computer forensics and incident response, and how to manage others to do practical computer forensics and incident response.

6.4 Ph.D. Course Structure

A student is qualified for Ph.D. studies if he/she has completed a M.Sc. with a research focus and have achieved at least a "B" on the master's thesis. A Ph.D. program requires at least 30 credits of coursework where at least 20 have to be at the 6000-level. Courses from this selection should generally be structured to allow advanced M.Sc. students the option to participate at the sole discretion of the instructor, provided they have established good academic standing in their regular courses.

We are currently establishing the following lecture-format courses providing a common infrastructure for several research areas; beyond this, most courses at this level are held as seminars, with additional informal (non-credited) reading groups supplementing specialized materials.

6.4.1 *Research Methodology*

This course encompasses general techniques for writing technical reports and research papers and also covers the rules, publication guidelines, and traditions with a particular emphasis on computer science and mathematical sub disciplines relevant to information security. Some aspects of the theory of science and epistemology as required to provide a solid foundation for the comprehension of the scientific method and also mathematical research techniques are also required. In addition, auxiliary information such as research and information retrieval is also covered while the course can only offer an overview of common research methods in computer science, software engineering, and mathematics; more detailed techniques are typically left to individual seminars.

6.4.2 *Computation Models and Complexity*

This course encompasses the core models and mechanisms required for the design and analysis of algorithms and particularly computational models. To this end, models of computation, Turing machines, recursive functions, Church's thesis, λ calculi, decidability, and computability, are covered.

Beyond this core, denotational semantics and the logic of programs are covered as well as applications to automata, formal languages, program verification, and programming languages. A final component of the course provides an overview of complexity theory including analytical techniques and an introduction to complexity hierarchies.

6.4.3 *Discrete Mathematics and Graph Theory*

This course covers applied aspects of discrete mathematics and graph theory as may be useful in modeling and analysis e□orts. To this end, the theory of graphs, including adjacency and incidence matrices, planarity, hamiltonian circuits, Euler's formula, directed graphs, and trees are covered along with the effciency of the known algorithms for performing various operations on graphs. In addition, optimization problems and techniques for networks, including single and multi-commodity network flow, critical paths are also covered in this course.

7. CONCLUSIONS

In this paper we have described some of the challenges and opportunities presented by offering a full spectrum of academic degrees from the B.Sc. to Ph.D. level solely in information security. Two concerns have had to be addressed for these e□orts to be successful. One was the ability to offer a clear progression in the depth and intensity of study of closely related subjects, particularly within the core curriculum of each degree program while still permitting students to enter (particularly at the M.Sc. stage and, to a lesser degree, at the Ph.D. level) without being placed at a marked disadvantage compared to students who have progressed linearly through the program. The second concern we had to address is the heterogeneity in the student population in which, again primarily at the M.Sc. level, students who have not had exposure to concerns outside higher education are taught together with mature students who, in some cases, may already have several years' worth of practical experience in information security and may hence approach their studies from an entirely different perspective.

We believe that the curricula we have described in this paper, along with the broad spectrum of delivery mechanisms and approaches, can both provide an academically challenging and professionally rewarding education which will enable students pursue or further careers in both academia and industry. However, it should be noted that there is as yet only a small data set to base observations of the success of graduates at the various levels. However, we intend to follow up with graduates longitudinally to track their assessment and feedback on the program as they progress to ensure that all programs remain both challenging and relevant to students.

8. REFERENCES

[1] L. Anderson and D. R. Krathwohl, editors. *A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's*

Taxonomy of Educational Objectives. Longman, New York, NY, USA, 2001.

[2] M. Bishop. Academia and education in information security: Four years later. In *Proceedings of the 4th Colloquium for Information Systems Security Education*, 2000.

[3] B. S. Bloom and D. R. Krathwohl, editors. *Taxonomy of Educational Objectives: The Classification of Educational Goals.* Longmans, Green & Co., New York, NY, USA, 1956.

[4] C. Ciechanowicz, K. M. Martin, F. Piper, and M. J. B. Robshaw. Ten years of information security masters programmes. In *World Conference on Information Security Education*, pages 215–230, 2003.

[5] CISR. Seventh workshop on education in computer security (wecs7). http://cisr.nps.edu/WECS7/. (Retrieved June 10. 2006).

[6] CISSE. Colloquium for information systems security education. http://cisse.info. (Retrieved June 10. 2006).

[7] G. Conti, J. M. D. Hill, S. Lathrop, K. Alford, and D. J. Ragsdale. Towards a comprehensive undergraduate information assurance program. In C. Irvine and H. Armstrong, editors, *Security Education and Critical Infrastructure*, pages 243–260. Kluwer Academic Publishers, 2003.

[8] D. Frincke and M. Bishop. Joining the Security Education Community. *IEEE Security & Privacy*, 2(5):61–63, Sept./Oct. 2004.

[9] M. Hentea, H. S. Dhillon, and M. Dhillon. Towards changes in information security education. *Journal of Information Technology Education*, 5:221–233, 2006.

[10] C. E. Irvine and H. L. Armstrong, editors. *Security Education and Critical Infrastructures, IFIP TC11 / WG11.8 Third Annual World Conference on Information Security Education (WISE3)*, June 26-28, 2003, Monterey, California, USA. Kluwer, 2003.

[11] N. P. Schembari. A bachelor of science degree in computer security: The experiences of a national center of academic excellence in information assurance education. In *Proceedings of the 9th Colloquium for Information Systems Security Education*, pages 6–11, 2005.

[12] C. Taylor, R. Shumba, and J. Walden. Computer security education: Past, present and future. In *Proceedings of the Seventh Workshop on Education in Computer Security (WECS7)*, pages 67–78, 2006.

[13] M. E. Whitman, editor. *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*, Kennesaw, GA, USA, Sept. 2005. ACM, ACM Press.

[14] M. E. Whitman and H. J. Mattord. A (draft) model curriculum for programs of study in information security and assurance. http://infosec.kennesaw.edu/presentations /InfoSecCurriculumModel.pdf. (Retrieved June 10. 2006).

[15] M. E. Whitman and H. J. Mattord. Designing and teaching information security curriculum. In *InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development*, pages 1–7, 2004.

[16] M. E. Whitman and A. Woszczynski, editors. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, Kennesaw, GA, USA, Oct. 2004. ACM, ACM Press.