Information Security Education at the Georgia Institute of Technology

Mustaque Ahamad* Seymour Goodman Wenke Lee Sham Navathe
Michael Nelson-Palmer Andre dos Santos H. Venkateswaran
Jim Xu
Georgia Tech Information Security Center
College of Computing
Georgia Institute of Technology
Atlanta, GA 30032

March 29, 2001

GENERAL SUBMISSION

Abstract

The Georgia Institute of Technology has recognized the importance of information security education and research by creating an interdisciplinary center called the Georgia Tech Information Security Center (GTISC). The educational goals of GTISC include the development of an information security curriculum that would serve students from a broad range of backgrounds. It takes an integrated approach to information security education that covers both technological and policy issues. A group of eight faculty from Georgia Tech has worked to create an innovative and broad curriculum that could be used to train future information security professional.

The curriculum design is motivated by several goals. First, the courses defined by it should be accessible to students that come from a broad range of backgrounds. At the same time, it should offer opportunities for students to specialize in various aspects of information security. The proposed curriculum starts with a gateway course that provides a broad introduction to the field. This is followed by an initial set of courses, each of which focuses on a coherent body of knowledge. Each course will introduce students to core concepts that cover a particular aspect of information security and will include projects that provide hands-on experience with the tools and techniques that can be used to build high assurance systems. It will be necessary to develop teaching materials and projects for the courses. The creation of such materials is a key component of our current work. A laboratory where the projects can be done in a controlled environment is also being developed by us. The curriculum will enable a variety of programs in the information security area for a diverse body of students. These include an undergraduate specialization, Masters' level programs and an information security concentration area for doctoral students. We hope that these programs will be able to meet the critical needs that exist for information security professionals.

*Contact author: Email – mustaq@cc.gatech.edu, Phone - (404) 894-2593)

1 Introduction

The Georgia Institute of Technology is a premier technological university that offers nationally ranked undergraduate and graduate degree programs in engineering, computing, and several other disciplines. Georgia Tech educates a diverse student body and enrolls approximately 11,000 undergraduate and 3,000 graduate students. Georgia Tech undergraduates are among the best in the nation (average SAT score of entering freshmen in 2000 was 1323) and the student body includes significant numbers of women and minorities. It has outstanding educational as well as research programs in a large number of technological disciplines.

Georgia Tech has long recognized the importance of information technology in our society. It created one of the first computer science departments in the country. In 1990, it created the College of Computing to promote computer science and information technology related education and research activities. In 1998, Georgia Tech established an interdisciplinary center called the Georgia Tech Information Security Center (GTISC). GTISC's mission is to become a leading research and development center, and to create a variety of educational opportunities in the information security area that prepare students for our information technology driven society. The College of Computing is the primary home of the educational offerings in information security. However, because of its interdisciplinary nature, many other units participate in both the educational and research activities of GTISC.

The College of Computing has established information security as an important area of growth. In addition to several existing faculty in related areas, we have hired several new faculty in recent years who have their primary research expertise in information security. The College plans to aggressively recruit additional faculty in this area to offer world-class education and research activities in the information security area. Although the College of Computing offers a rich computer science curriculum and courses in a number of interdisciplinary areas, our current educational offerings are quite limited in the information security area. To meet GTISC's educational mission, we are developing a broad and innovative curriculum that covers various facets of information security.

Section 2 outlines the goals that must be met by the information security curriculum that is being developed by us. Section 3 discusses a teaching laboratory that is being developed. Section 4 presents a a list of courses that make up the curriculum, and plans for the development of the courses. Section 5 briefly discusses related efforts. The paper concludes with biographical sketches of the authors.

2 Curriculum Goals

Our primary objective is to develop an innovative curriculum that covers both core concepts of the information security area and provides hands on experience with the tools and techniques that exist for building high assurance computer and network environments. At the same time, we take a broad view of the information security problem and claim that both technological and policy issues must be addressed in an integrated manner to train well prepared information security professionals. The development of our curriculum is driven by the following goals.

1. We believe that a strong information security curriculum should build on a solid background in computer science. At the same time, we feel that information security technology and policy

issues extend well beyond traditional computer science programs. Many future information security professionals could come from backgrounds that are not in computer science. Because of these reasons, we believe that the curriculum should be designed in such a way that it is accessible to students from a broad set of majors. In addition to Computer Science majors at Georgia Tech, we expect students majoring in Computer Engineering, Public Policy and International Affairs, and College of Management to take one or more of the courses.

2. A well rounded information security program graduate should not only have a solid understanding of technological solutions but the viability and costs of such solutions in the context of their public policy implications. These issues are complex because the critical infrastructure spans national borders and many policy issues are international in nature. Thus, the curriculum should address both technology and policy aspects of information security in an integrated manner.

3. The curriculum should have the breadth and depth to meet the needs of a variety of students. Thus, with proper choice of courses, it should be possible for undergraduate students to specialize in information security. The curriculum should be rich enough to offer specialization at the graduate level as well. In particular, it should be feasible to design a certificate program in information security for Computer Science M.S. students, and a Masters degree program in information security. At the same time, doctoral students who plan to do their dissertation research in information security should be able to acquire the necessary breadth and depth by taking the courses that are developed by us. We already have many doctoral students who plan to work in information security related area. The new curriculum should enable us to train them for successful careers in education and research.

4. Finally, the curriculum should incorporate hands-on projects in information security and provide significant experience with the tools and techniques that could be used to build high assurance systems.

A curriculum that supports the multiple goals we outlined above requires the design of a rich set of courses, instructional materials for these courses, and laboratory facilities where hands-on projects associated with the courses can be done. Of course, a specialized program such as the one proposed here requires faculty who are interested in the many aspects of information security. We are fortunate to have such a group of faculty who have worked on the curriculum design and implementation. We discuss the information security programs and the information security teaching laboratory, followed by the courses and the body of knowledge covered by them. We also discuss the materials that will be necessary for the successful delivery of these courses.

2.1 Information Security Programs

The curriculum being developed by us allows students to define an information security concentration both at the undergraduate and graduate level. At the undergraduate level, Georgia Tech allows students to choose specialization areas. They must take several junior and/or senior level courses in the chosen area. By choosing a subset of these courses in the new curriculum, it will be possible to define a specialization at the undergraduate level in Information Security. The students who choose this specialization will have significant knowledge and understanding of the information security field to fill workforce needs in the area of critical infrastructure protection.

At the graduate level, the curriculum will allow us to offer information security concentrations both at the Masters and Doctoral levels. At the Masters level, we plan to offer a certificate and/or a degree program in information security. The curriculum must include courses that are needed to support such programs. At the PhD level, students must choose a concentration area and take several courses in it to gain breadth as well as depth in their chosen field. The proposed curriculum will permit doctoral students to achieve this breadth and depth in the information security field which is currently not possible. We already have many doctoral students who are pursuing their dissertation in the information security area. They are forced to declare concentrations in other areas because of the lack of courses such as the ones proposed here.

Our goal is to define an innovative and broad curriculum and implement it so that a large number of students can benefit from it. We have ample evidence of student demand for our information security programs. Several exploratory courses that have been taught by us in information security have been full and they have attracted students from several majors.

3 Information Security Teaching Laboratory

Several of the courses that we have developed include project work that provides hands-on experience to students. One laboratory course will be entirely based on projects that explore the use of tools and techniques that can be used to defend information systems against a variety of attacks. A range of projects that explore vulnerabilities of such platforms as well as defense techniques are being defined and will be used to teach the concepts covered in the courses.

To facilitate the inclusion of non-trivial projects in information security courses, we are setting up a dedicated laboratory for instruction purposes. Although some projects can be completed with general laboratory facilities, many of them require access to packages that are not installed on general purpose and publicly shared computer systems. We are creating a stand alone teaching laboratory that has minimal connectivity to external networks. This laboratory will house a variety of hardware and software platforms, including network routers. The space for a teaching laboratory for information security has already been committed and we are building the necessary infrastructure for this laboratory.

4 A Broad Information Security Curriculum

A number of universities offer several courses that cover material from the information security and assurance areas. We have also taught several "exploratory" topics courses in the information security area in the past two years. Although we studied the courses offered elsewhere carefully and benefited from their as well as our own experiences, the goal of a broad curriculum that can be used to train both undergraduate and graduate students from various backgrounds has motivated us to take a fresh approach to the design of an information security curriculum. Our design also allows for augmenting the curriculum with courses that can be taken to specialize in various facets of information security.

We have tried to identify the core body of knowledge for a broad information security curriculum and its packaging in a set of courses that can be taught at Georgia Tech. For each course, we are developing the necessary materials for instruction, evaluation and laboratory projects that will

provide hands-on training with the tools and techniques that can be used to secure information systems. Below, we discuss an initial set of courses that we have designed as part of this effort. In particular, we discuss course objectives and learning goals, as well as the topics that make up a coherent body of knowledge that should be covered in each course. This is followed by a discussion of instructional materials that will make up the portfolios of the courses.

The courses discussed below are based on our initial planning and reflect the expertise our faculty has in the information security area at this time. We expect this list to grow based on student interests and as our information security faculty grows. We have also identified existing courses in the Mathematics department that focus on theoretical foundations of cryptography. Other relevant courses from the College of Management that deal with risk analysis and management are also being identified. We plan to explore synergistic relationships across these courses.

4.1 New Information Security Courses

1. Introduction to Information Security

Prerequisites: This gateway course provides the essential background to students of different majors so they can go on and take other courses in the information security curriculum. Thus, this course should be accessible to students that come from computer science, engineering or programs such as international affairs, public policy and management. The course requires senior undergraduate or graduate standing, and some background and familiarity with computer systems.

Learning Objectives: This foundation course provides a broad overview of the field of information security. It will help students coming from several majors, undergraduate or graduate, understand this important topic as it relates both to their field of study and their personal knowledge about information systems vulnerabilities. The primary objectives of the course are to (1) understand the importance of information security and how it affects our interconnected network world, (2) identify the key areas of information security and how they "work", and (3) learn how to critically analyze situations of information system use to identify the magnitude of security problems, possible options for resolution, and probable consequences of actions.

Body of knowledge: From the macro perspective, the course would cover several basic areas. The first topic is key definitions and terms such as information operations, information security and information assurance. The second topic would touch on the problems and issues surrounding the private citizens' concern for privacy. The next topic would be the impact of laws and public policy as it relates to national problem of critical infrastructure protection. The fourth topic is the key, but difficult, nature of information security in overall business or organizational risk.

From a technical perspective, the course also would touch on key basic areas. The first topic would be an establishment of a common understanding of key fundamental concepts, definitions, and terms such as security goals, threats, vulnerabilities, controls and principles of information systems security. The rest of the technical focus of the course would be to examine the important dimension of providing security for information processing systems-general and secure operating systems, applications, databases, networks and distributed systems, cryptography, and security protocols.

Development Plan: The plan covers seven phases or elements. First, it is necessary to select text(s) that adequately cover the broad range of topics such that the content is accessible to

students from many different backgrounds. The course topics need to be arranged in a coherent and understandable manner. The topics need to make sense to students with less of a technical background but should allow technically savvy students to explore them in more detail. Some topics will stand alone in their mention and emphasis. Other topics will be the foundation information for the follow-on courses in the program. We need to identify the necessary level of depth for the various topics as the overall curriculum is developed. Finally, we are developing homeworks and projects that are appropriate for students that come from mixed background. The homeworks and projects should reinforce and clarify broad range of topics covered by the class. The projects should allow groups of diverse students to explore many aspects of a secure information system.

2. Applied Cryptography

Prerequisites: This course requires senior undergraduate or graduate level standing. It also requires a course in discrete mathematics and strong programming skills.

Learning Objectives: Cryptographic techniques are used widely to protect information when it is transmitted over open networks. At the same time, protocols such as digital signatures require a solid understanding of the underlying cryptographic techniques. The primary objective of this course is to provide such an understanding, while focusing on the application of the cryptographic techniques. In particular, the course introduces students to both symmetric and public key cryptographic systems and protocols based on them. The students also learn how to analyze cryptographic protocols to identify their weakness in certain environments.

Body of Knowledge: The course starts with the basics of the mathematics relevant to the understanding of cryptographic techniques, particularly in number theory and elliptic curves. After providing the necessary background and some discussion of classical cryptographic techniques and cryptanalysis, the course discusses in detail symmetric as well as public key based cryptographic algorithms. Algorithms such as DES, 3DES, MARS, RC4, Twofish, AES, Diffie-Hellman, RSA and others are covered in details. The course also addresses elliptic curve cryptography and digital signatures and hash and MAC functions. Practical issues such as certificates, key distribution and public key infrastructures are introduced. Finally, a variety of cryptographic protocols such as Clipper chip, SSL/TLS, S/MIME, SET, PGP, PPTP, GSM and WEP, and applications based on them are analyzed in detail.

Development Plan: Although several textbooks exist from which material covered in this class can be drawn, the development of good homeworks, projects and instructional material that focuses on the application of cryptographic techniques to build protocols that address practical problems will require considerable effort. At the same time, we want to identify and catalogue domain specific application scenarios (e.g., online banking) that help students understand what aspects of security can and cannot be addressed by cryptographic protocols alone.

3. Secure Computer Systems

Prerequisites: This course assumes that students have taken undergraduate level operating systems and database courses.

Learning objectives: Applications are enabled by software systems such as operating systems and databases. Thus, the secure execution of such applications depends on what trust assumptions

can be made about the underlying systems. At the same time, by providing right mechanisms for protecting information and other resources, operating systems can facilitate and encourage the development of secure applications. An integrated approach to secure operating systems and databases is attractive because both types of systems share many common mechanisms to mediate access to protected information.

The main objective of this course is to study the threats and vulnerabilities that should be addressed at the operating systems and database levels. There is a significant body of knowledge that exists in this area and students will be introduced to it. They will gain a solid understanding of the techniques that have been developed for building secure operating systems and databases. By doing projects that provide experience with real systems and applications, students will gain an appreciation for what must be ensured by underlying software systems to facilitate secure execution of applications.

Body of Knowledge: The course starts with the problem of how to characterize a trusted computing system. Students explore the Orange Book trusted computer evaluation criteria as well as the common criteria to understand the functionality expected from a secure system. The course also covers general design principles of secure computer systems (e.g., least privilege) and then explores in detail the problems of authentication, authorization and audit. The interactions between the operating and the database systems and their respective roles in providing secure transactions are discussed. Various access control models that include discretionary and mandatory access control are studied. Solutions prevalent in secure databases such as polyinstantiation of data, multilevel secure indexes etc. are discussed. The operating system level mechanisms such as security kernels, access control lists and capabilities and their implementations are also investigated in detail. In particular, the course explores Multics rings, Hydra's capabilities and the Java access control model. The course also introduces threats such as Trojan horses, viruses and covert channels and the measures against them. Extensions of database access primitives for security and extensions to SQL for authentication are discussed. Where possible, real systems are used to illustrate the security mechanisms and policies offered by them, and the potential vulnerabilities that could exist when the mechanisms are used improperly.

Development Plan: The material covered by the topics in this course comes from a variety of sources that include reports, research papers and even some textbooks. Furthermore, the integration of operating systems and database material so that the basic protection mechanisms and security policies can be presented in a unified manner is also challenging. We plan to undertake the selection, collection and presentation of the relevant material and develop a coherent set of topics for this class. At the same time, we plan to develop challenging homeworks and project assignments that will allow students to gain practical experience with real systems. For example, one can develop a project where students define and implement a security policy using Java access control model. Such a policy will control and restrict access to local resources to code that comes from foreign hosts. Other Linux based projects are also being developed.

4. Network Security

Prerequisites: Students are expected to have a solid grasp of the fundamentals of computer networking, including a basic understanding of the operation of the protocols in the TCP/IP suite, especially IP. It is also assumed that students have taken a course equivalent to "Applied Cryptography". In addition, students are expected to have a level of mathematical maturity that

includes basic algebra and the ability to learn and use new mathematical notations. Some C programming ability is essential, as we will be looking at implementations of several protocols.

Learning objectives: With the rapid growth of the Internet, security becomes one of the most important aspects of computer networks. Many inter-net protocols and applications were designed with minimal attention paid to issues of confidentiality, authentication, and privacy. As our daily activities become more and more reliant upon data networks, the understanding of such security issues becomes more and more critical. This course provides an introduction to the topic of security in the context of computer networks. It is intended for graduate students who have some understanding of networks, but not necessarily a significant background in information security. The goal of the course is to provide students with a foundation allowing them to identify, analyze, and perhaps solve network-related security problems in computer systems. The course covers fundamentals of authentication, and the use of encryption technologies in secure network communication, as well as the practical problems that have to be addressed in order to make those technologies viable in a networked environment, in particular in the Internet environment.

Body of Knowledge: This course focuses on information security at the network level. Thus, it explores security requirements such as confidentiality, integrity, authentication, and privacy in the context of networks and communication systems. It addresses the role and importance of a network and system security policies and network-related security threats and countermeasures. Firewalls are covered in detail. Principles of security protocols, with Internet Protocol security architecture (IPSEC) as an example, are also covered. Finally, intrusion detection principles and architectures, information protection and digital watermarking and other related topics are discussed.

Development Plan: Several textbooks exist that cover many of the topics listed earlier. We are developing a sequence of homeworks and projects that allow the students to gain a deep understanding of the topics covered in this class. Such homeworks and projects should help students apply what they have learned from the lectures to (1) analyze security protocols for weaknesses, (2) design and/or implement an network authentication protocol for a given set of constraints, or (3) design and/or implement an encryption system.

5. Formal Models and Methods for Information Assurance:

Prerequisites: This course assumes background knowledge from theory of computation covering basic automata theory and algorithms. A course equivalent to "Introduction to Information Security" is also required to ensure that students have a basic understanding of information security and assurance.

Learning Objectives: To gain an understanding of the formal models and methods that can be applied in constructing high assurance systems. This requires a solid understanding of concepts such as equivalence checking, model checking, and theorem proving, and models such as Petri nets, state charts, and temporal logic. These formal methods are applied to model and reason about information security problems such as authorization and authentication. The students also study the viability as well as limitations of formal verification methods for building high assurance systems. The course also provides exposure to algorithmic tools useful for modeling and analysis of high assurance systems.

Body of Knowledge: The course starts with logical foundations which include the basics of propositional, predicate and temporal logics. It also discusses model checking, theorem proving and

the applications of these techniques for verifying the correctness of protocols and programs. These techniques are then applied to explore several protocols from the information security domain. These include authorization, authentication and trust models. The course also explores formal exposition of security policies, information flow and certification and verification of high assurance software. Students are exposed to advanced topics in the field.

Development Plan: The development of this course is a challenging task because techniques from the formal models and methods area should be taught in the context of information security and software engineering. Thus, it is necessary to integrate material from several sources, including textbooks on logics and their applications, and research papers that apply the logics to problems in information security. For example, material from research papers can be used to illustrate how a formal logic can be used to specify and understand complex authentication protocols in distributed environments. We plan to explore such connections for a wide range of information security problems. We are also developing innovative homeworks and projects that further reinforce the integration of formal methods and their application to secure systems.

6. Information Security Laboratory:

Prerequisites: Secure Computer Systems, Network Security and strong programming skills.

Learning Objectives: Current computer networks and systems are vulnerable to many different attacks. The explosion in the use of the Internet has aggravated the problem of unauthorized use of network and computer resources via a range of attacks, including the so called denial-of-service attacks. The goal of this course is to provide hands on experience with tools and techniques that can be used to defend computer systems against a variety of attacks. The laboratory has been designed to be easily configured to express real-world organizations and networks as needed. A particular configuration provides students with the ability of getting an inside view of what can happen on the target configuration, while doing this in a controlled environment. In particular, students can gain an understanding of how to identify vulnerabilities, the results when they are exploited by attacks, and the methods that can be used to defend against such attacks. This is done with heterogeneous software and hardware platforms, by studying the different vulnerabilities that exist within each and across them.

The laboratory will allow students to gain experience with tools and methods that can be used to strengthen the security of networked systems. Thus, the laboratory course will train students to understand what vulnerabilities are; how to protect against attacks that exploit them; and how to deal with adversaries that have various levels of expertise and familiarity with the installations that need to be secured.

Body of Knowledge: This course explores the vulnerabilities existing in operating systems, applications and specifications of various protocols and their implementations. Students will become familiar with the tools that are used for attack/defense and how they can be employed to build secure systems. At the same time, they will learn to analyze systems for their vulnerabilities and how to counteract possibly malicious acts. Audit techniques that allow one to detect unauthorized penetrations are also studied.

Development Plan: This course is the most challenging to design because of a number of reasons. First, one must classify and catalogue vulnerabilities in several hardware and software platforms and study the attacks that exploit these vulnerabilities. This should be followed by characterizations

of tools and techniques that are used to counter attacks that can be mounted against the systems. Ideally, teams of students can work with or against each other in projects that involve penetration, detection and defense against various attacks. Thus, this project driven class provides real hands-on experience in actively defending information systems against a variety of attacks. Students are able to experiment with an isolated network that mirrors real organizations without accessing systems outside of the laboratory. The students are also taught ethical issues related to attack/defense of computer systems.

7. Information Security Strategies and Policies

Pre-requisite: Introduction to Information Security.

Learning Objectives: Outside of the narrow technical R&D domain, information security has to exist in the context of an organization or population. These are the owners and users of the vulnerable systems and information, and ultimately it is they who suffer from the threats and loss. These entities exist at many different levels, ranging from the individual and the home, through the mid-level unit of a company or government agency, through national and international organizations and populations. All have to balance the trade-off of the costs incurred with the desire for greater security - direct monetary and personnel costs, decreased efficiencies and access, possible degradation of other missions and values (e.g., privacy) - against the benefits of greater security. For most decision-makers, few of these choices are binary, but complex compromises are generally both necessary and possible, and these must be done within legal or other constraints. Many of these choices, including choices among the technical and procedural means for achieving desired levels of security, have to be tailored to the organizations and populations at risk. Strategies and policies must be formulated to define and achieve these goals. Policies explicitly state what may, should, and should not be done. Management, political leadership, and the technical community must work together to make effective strategy and policy.

The macro-goal of this course is to infuse the students with this viewpoint. Most of the time and effort spent within the course will be devoted to a taxonomy of the issues at all levels, and educating the students to participate in the determination of appropriate strategies and policies.

Body of Knowledge: Most of the content is partitioned between two levels: the company or government agency, and the national and international. For both levels, we consider the determination of vulnerabilities and risks; a taxonomy of competing priorities and factors in the provision of security; legal, cost, and other constraints; the derivation of strategies; and the technical and procedural means to achieve the desired ends. At the firm level, some focus is given on how to achieve effective, but minimally intrusive, security. At the national and international levels, we include studies of issues related to law enforcement, forms of active defense, national security, regulation to achieve desired levels of security, responsibility and liability, privacy, the harmonization of differences in perspectives and laws between countries, and the assurance and protection of very large IT-based infrastructures.

Development Plan: Georgia Tech is well positioned to make this the premier courses of its kind in the United States. This follows from the number, quality, and experience of the faculty we have on-campus with an interest in this subject. In addition to Prof. Goodman, we plan to involve several faculty members in the design and delivery of this course. Georgia Tech President Wayne Clough is co-chairman of the national Internet Policy Institute. Prof. Stephen Lukasik was deputy director and then director of ARPA when the ARPANET was created, and then Chief Scientist of

the FCC, before going on to related senior executive positions in industry. Among other things, both Profs. Goodman and Lukasik were included in the few acknowledged advisors to the Presidential Commission on Critical Infrastructure Protection, and continue to work extensively on national and international IT-related security issues. Prof. Deborah Johnson of the School of Public Policy is an authority on technology-related ethical issues. Prof. Hans Klein of the School of Public Policy is President of Computer Professionals for Social Responsibility and works extensively on issues of Internet governance and privacy. Finally, recently retired Senator (and now Professor) Sam Nunn, the senior member of Congress heading the board overseeing the President's CCIP and a primary mover behind establishing the GTISC, retains very strong interests in this subject.

5 Related Efforts

There has been considerable discussion about information security education [1-6]. Also, there are several Computer Science departments that currently offer courses in the information security area, including concentrations such as certificates in this area. Examples of such departments include University of California at Davis, Naval Postgraduate School, George Mason University, Purdue University and others. We have carefully studied the curriculum that is offered by these departments and have benefited from the information that has been available. We will seek feedback and share our experiences with others as the curriculum is implemented at Georgia Tech.

References

[1] Steve Barnett. Computer Security Training and Education: A Needs Analysis. In Proceedings of the IEEE Symposium on Security and Privacy, May 1996.

[2] Shiu-Kai Chin, Cynthia Irvine and Deborah Frincke. An Information Security Education Initiative for Engineering and Computer Science, Technical Report NP SCS-97-003, Naval Postgraduate School, December 1997.

[3] Heather Hinton. Review of the First Annual Workshop on Education in Computer Security. Electronic CIPHER, Issue 21, March 1997.

[4] Cynthia E. Irvine. Goals of Computer Security Education. In Proceedings of IEEE Symposium on Privacy and Security, May 1996.

[5] Cynthia Irvine, Daniel Warren and Paul Clark. The NPS CISR Graduate Program in INFOSEC: Six Years of Experience. In Proc. of 20th National Information Systems Security Conference, October 1997.

[6] John Kauza. Industrial Perspective on INFOSEC Education Requirements. In Proceedings of the National Colloquium for Information Systems Security Education, April 1997.

Participating Faculty

The curriculum has been developed by a group of faculty who are interested in the information security field. This group, which consists of seven tenure-track faculty and one instructor, has the following members.

1. Mustaque Ahamad is a Professor of Computer Science in the College of Computing. He received his PhD from the State University of New York, Stony Brook, in 1985. His research interests are in operating systems and distributed systems. He has active NSF funded research projects in the information security area which are developing security services for large scale and ubiquitous computing environments. In particular, he is exploring sensor-based parameterized authentication in ubiquitous environments and access control models that allow access based on the context in which requests are made.

2. Seymour E. Goodman holds a joint appointment in the Sam Nunn School of International Affairs and the College of Computing at Georgia Tech where he is a professor. He received his PhD from the California Institute of Technology. He works on a variety of projects that focus on policy side of securing the critical infrastructure. He has also done considerable work on the diffusion of the Internet.

3. Wenke Lee will join the faculty of the College of Computing as an Assistant Professor in August 2001. He received his PhD from Columbia University in 1999. His research interest focus on intrusion detection techniques.

4. Sham Navathe is a Professor of Computer Science in the College of Computing. He received his PhD from the University of Michigan. His research interests are in database systems. He has done work in secure databases in the past and has authored a well known textbook in the database area.

5. Andre dos Santos is an Assistant Professor in the College of Computing. He received his PhD in 2000 from the University of California, Santa Barbara, where he worked with Richard Kemmerer. His research interests cover a range of information security areas, including identification of vulnerabilities in application and systems, smart cards and design of secure distributed systems and applications.

6. H. Venkateswaran is an Associate Professor of Computer Science in the College of Computing. His research interests are in theoretical computer science. In the past, he has worked on formal models and their applications in complexity theory. He is interested in the application of such formal models for information assurance.

7. Jun Xu is an Assistant Professor in the College of Computing. He received his PhD degree in 2000 from Ohio State University. His research interests are in networks and network security. He is particularly interested in high speed firewalls, intrusion detection and countering denial-of-service attacks.

8. Mr. Michael Nelson-Palmer is retired from the U.S. Army. He is an instructor in the College of Computing. He got his M.S. from the Naval Postgraduate Schools and has experience with information security problems in several different defense environments.