THE NPS CISR GRADUATE PROGRAM IN INFOSEC: SIX YEARS OF EXPERIENCE

Cynthia E. Irvine, Daniel F. Warren, and Paul C. Clark

Naval Postgraduate School
Department of Computer Science
Code CS/Ic (CS/Wd, CS)
Monterey, California 93943-5118
Email: irvine(warren, clarkp)@cs.nps.navy.mil

Abstract

The Naval Postgraduate School Center for Information Systems Security (INFOSEC) Studies and Research (NPS CISR) is developing a comprehensive program in INFOSEC education and research that can become a resource for DoN/DoD and U.S Government in terms of educational materials and research. A security track within the Computer Science curriculum at the Naval Postgraduate School has been established. Building upon a foundation of computer science laid by the department's core curriculum, the security track conveys vital concepts and techniques associated with INFOSEC today.

KEYWORDS: INFOSEC, Education

1 Introduction

A recent Defense Science Board [1] study cited the need for broader and deeper education in the building of resilient systems so that key aspects of the information infrastructure could be more secure. In particular, the task force noted that to address the challenge of information warfare, a cadre of computer scientists with MS and Ph.D. degrees with specialization in Information Systems Security (INFOSEC) is needed. The study recommended curriculum development at the undergraduate and graduate levels in resilient system design practices.

Over the past six years, the Naval Postgraduate School (NPS) has developed a coherent educational program in INFOSEC education. This effort is under the umbrella of the Naval Postgraduate School Center for Information Systems Security Studies and Research and Research (NPS CISR). This paper describes the programs and structure of the graduate education program at NPS CISR. First we will establish the context and objectives of the program. Then details regarding the curriculum will be described.

2 Background

2.1 Computer Science at NPS

The INFOSEC education program at NPS is part of the Computer Science Curriculum. In the two-year, eight-quarter Masters degree program, students are required to demonstrate competence in a core curriculum of traditional

computer science courses. Many entering students have no prior education in computer science. They must cover the fundamentals of computer science which include the theory of formal languages, computer systems principles, object-oriented programming, data structures, artificial intelligence, operating systems, software methodology, database systems, computer communications and networks, computer graphics or interactive computation, computer security, and the design and analysis of algorithms.

To allow for specialization in a variety of areas, the core curriculum is enhanced with tracks in the following areas: software engineering; artificial intelligence and robotics; database and data engineering; computer graphics and visual simulation; computer systems and architecture; and computer security.

Each student's course of study is capped by a written thesis, most often based on research directed by a faculty member in the student's chosen specialization track. This work must be conducted during the sixth through eighth quarters in conjunction with classes. In many cases students start thesis research prior to the sixth quarter.

Thesis research has several benefits for the student: it allows them to be involved in work addressing an unsolved problem, usually within the framework of the DoD or U.S. Government; it enhances both their oral and written presentation skills, and it hones their critical thinking abilities.

2.2 NPS CISR

The computer security track was established in 1991 to address the growing need for INFOSEC education of U.S. military officers. Initially, a successful, two-course sequence in INFOSEC was launched: an introductory course and an advanced topics course. In 1994 it was recognized that two courses were inadequate to cover all aspects needed for graduates to address complex INFOSEC issues. The track was expanded and new INFOSEC courses were added to the Computer Science Curriculum.

As laboratory resources and sponsored research on INFOSEC topics grew, it became apparent that the effort was more than just a series of classes. With the encouragement of sponsors, the Naval Postgraduate School Center for INFOSEC Studies and Research (NPS CISR) was officially established in October 1996. Today, NPS CISR involves the research of eight faculty and staff members, nine thesis students, and approximately 150 students participating in classes and laboratory work annually. Students in Computer Science, Information Technology Management, and Information Warfare curricula all take courses in computer security.

NPS CISR serves the INFOSEC research and education needs of DoD/DoN in seven primary areas.

- Curriculum development ensures that a coherent and comprehensive program in INFOSEC foundations and technology is presented at the university and postgraduate levels.
- Development of the INFOSEC and Trusted Systems Laboratory supports the INFOSEC teaching and research programs at NPS.
- Faculty development fosters the insertion of INFOSEC concepts at appropriate points in general computer science courses and involves interested faculty members in leading-edge INFOSEC research problems.
- A Visiting Professor program which brings INFOSEC experts to NPS to offer courses and engage in research with faculty and students.

- An Invited Lecture series injects commercial and military relevance into the NPS CISR activities.
- An academic outreach program permits other, non-CISR academic institutions to benefit from the INFOSEC education and research developments at NPS.
- An effort to insure that NPS CISR graduates are identified so that their expertise can be applied to the wide variety of INFOSEC challenges in DoD and U.S. Government.

Research, focusing on INFOSEC problems, with emphasis on those of DoN, DoD, and U.S. Government, is intended to be a major by-product of this effort.

3 Curriculum Objectives

The curriculum for the INFOSEC track has been designed to meet the following general objectives:

- To provide courses for both beginning and advanced students,
- To provide courses accessible by students who are not in the Computer Science curriculum,
- To insure that Computer Science students have a strong foundation upon which to base advanced course work in computer science and INFOSEC,
- To involve students in ongoing research and technology development efforts associated with computer security and INFOSEC,
- To enhance students' laboratory experience through the hands-on use of secure systems, and
- To heighten awareness of security issues with non-computer science majors, such as those studying management or procurement.

3.1 Course Content

In terms of content, we believe that it is essential that students understand the fundamental concepts behind risk avoidance as articulated in the Reference Monitor Concept [3]. This encompasses a notion of completeness that is absent from more intuitive and/or *ad hoc* approaches to computer security. The idea that a policy enforcement mechanism is always invoked, cannot be modified by unauthorized individuals, and is inspectable so that one can assess whether or not it works correctly is applicable over a broad range of security policies and mechanisms. This allows us to pursue a theory of computer security [5] and a corresponding engineering discipline. This also demonstrates that it is possible to design systems which are less susceptible to recurrent cycles of penetrations and patches [12].

In addition, our students must know how to function in the real world, where risk management techniques are employed [2]. The practical nature of these approaches make them attractive in situations where more complete systems are not in place. (Note that we are making a distinction between the study of these protection functions and system maintenance.) In addition, issues associated with the incremental achievement of security objectives are discussed.

Topics have been identified which we believe should be covered in an INFOSEC education program. Our position as a DoD university is reflected in some of these subjects, however, most are universal. They include, in no particular order: Risk Analysis, Disaster Recovery, Access Controls and Authentication, System Maintenance, Cryptography, Emanations Security, Audit Management, Protocols, Key Management, Configuration Management and Backups, Privacy Issues, User Monitoring, Personnel

Issues, Physical Security. Additional topics are covered as needed. Coverage in the introductory survey courses, by necessity, must be broad rather than deep, but the survey must provide sufficient technical depth to serve as a springboard for progressing to advanced studies.

Advanced courses can provide focused coverage of specific topics such as security policies and formal models, database security, security engineering, and network security. Seminar courses afford opportunities for advanced students to read and discuss current research areas in computer security. Electives drawn from other departments, such as mathematics and electrical engineering, permit students to explore subjects such as cryptography or emanations security in greater depth.

Care has been taken to integrate the INFOSEC courses into a coherent sequence. By avoiding compartmentalization within courses, students gain a progressively deeper understanding of many principles and techniques that span various areas of computer security. This foundation prepares students to address research and operational problems in INFOSEC after graduation. Through the use of case studies, students understand how past problems have been solved and have an opportunity to consider current topics.

3.2 Lab Requirements

The ultimate objective of all INFOSEC studies is to improve security in real systems. Thus, practical laboratory experience is crucial for an effective INFOSEC program. Laboratory exercises in the form of tutorials and projects help to reinforce and extend concepts conveyed in lectures as well as help prepare students for effective thesis research.

Most NPS CISR courses include a lab component. As existing courses are refined and new ones developed, corresponding lab exercises are prepared or updated. An objective of the NPS CISR program is to allow students to understand the kinds of technologies that are available to solve current computer security problems and to consider potential future technologies. Students are given first-hand experience in using a variety of trusted systems and explore topics in security policy enforcement, security technology for database systems, monolithic and networked trusted computing techniques, and tools to support the development of trusted systems.

4 INFOSEC Curriculum

Current courses in the NPS CISR program are described below. Their integration into the Computer Science curriculum is illustrated in Table 1. It is worth noting that our expanded program is still young and several of the courses are still in experimental stages.

4.1 Basic Courses

Two courses, Introduction to Computer Security and Management of Secure Systems, provide the survey of INFOSEC principles and techniques identified in the previous section. They are intended for the advanced undergraduate/beginning graduate level. The two courses review both the conceptually complete and more intuitive approaches to INFOSEC. These provide the students with an appreciation of both foundational concepts and current practice in computer security. The courses are updated quarterly to insure that topics associated with evolving technology and emerging DoN/DoD requirements are incorporated.

4.1.1 Introduction to Computer Security

Over time, we have made significant changes to the NPS CISR flagship course, Introduction to Computer Security. When initially offered, it was an upper level graduate course and had daunting prerequisites: data structures, software system design, networks, databases, and software methodology. In 1995, it was modified to be an intermediate rather than an upper-level graduate course.

A challenge in any educational program, and certainly in any survey course, is to present the material so that students are motivated to learn what initially appear to be a large collection of disjoint concepts, only to learn much later that these ideas can be synthesized into a larger framework. Significant reorganization of the course material in 1996 resulted in a presentation in which the rationale for each topic covered was more clear to the students during the course [10]. Several benefits accrue from this change. With fewer prerequisites, the course is accessible by a much larger population of NPS students. This results in an increased number of DoD personnel having taken a graduate-level INFOSEC course. In addition, it may be taken much earlier in each students' course of study. Thus students are "sensitized" to INFOSEC issues early. For computer science students, this means that they will have a better appreciation of how various areas of computer science such as operating systems, software engineering, and many of the more formal courses contribute to system security. For students in other curricula, this early overview of INFOSEC concepts permits them to understand how these ideas are applicable within their own discipline and affords them the opportunity to take more advanced INFOSEC courses as electives.

The second major change to Introduction to Computer Security was the injection of extensive laboratory material. Originally conceived with no laboratory component, now we have developed a set of laboratory exercises and tutorials which complement lecture material. A few topics are: passwords, discretionary access controls, mandatory access controls, exploitation of flaws in low assurance systems, exfiltration of sensitive information, and use of cryptography. Student feedback has been very positive as these exercises help to reinforce concepts discussed in lectures and give concrete examples of security implementations. In addition, students become familiar with a range of trusted products and security enhancements to untrusted systems. These include both high and low assurance trusted systems.

In 1996, over 150 students used the INFOSEC and Trusted Systems Laboratory for class assignments and laboratory exercises.

Catalog description

This course is concerned with fundamental principles of computer and communications security for modern monolithic and distributed systems. It covers privacy concerns, data secrecy and integrity issues, as well as DoD security policy. Security mechanisms introduced will include access mediation, cryptography, authentication protocols, and multilevel secure systems. Students will be introduced to a broad range of security concerns including both environmental as well as computational security. Laboratory facilities will be used to introduce students to a variety of security-related technologies including, discretionary access controls in Class C2 systems, mandatory access controls in both low and high assurance systems, identification and authentication protocols, the use of cryptography in distributed systems, and database technology in trusted systems.

4.1.2 Management of Secure Systems

With the changes adopted to Introduction to Computer Security, it was evident that one 12-week quarter was inadequate to survey all of the INFOSEC areas pertinent to DoD. Thus a complementary course, Management of Secure Systems, was developed.

A significant portion of the course is devoted to laboratory and field exercises. Risk analysis, certification and accreditation, system maintenance tools, and organizational aspects of INFOSEC are among the topics for lab activities.

Catalog description

This course is intended to provide students with an understanding of management concerns associated with computer-based information systems. Students will examine the security concerns associated with managing a computer facility. The impact of configuration management on system security, the introduction of software that must be trusted with respect to computer policies, environmental considerations, and the problems associated with transitions to new systems and technology will be studied in the context of Federal Government and especially DoD information systems.

4.2 Advanced Courses

The descriptions for these courses given here are less detailed and are intended to convey the overall objectives of each course

4.2.1 Applying INFOSEC Systems (Network Security)

This course presents topics in network security for both open systems and military/intelligence networks. Students review the cryptography and protocols commonly employed in networked systems. Approaches to key management in small and large scale enterprises are explored. Case studies allow students to understand the complexity of applying these techniques to DoN, DoD, and Government systems.

4.2.2 Advanced Computer Security (Database Security emphasis)

This course is evolving so that its area of emphasis will be database security. this will include not only traditional database security, but issues associated with workflow and transaction processing.

4.2.3 Secure Systems

This course is intended to provide students with an in depth understanding of the principles and techniques employed in building secure systems. Starting with fundamental concepts associated with protection in information systems [11]. Students will learn how software engineering principles such as modularity and layering, minimization, configuration management, the fault hypothesis method, and other techniques can be used to build secure and resilient systems.

4.2.4 Policies, Models, and Formal Methods

Policies, Models and Formal Methods covers the methods used to specify, model, and verify computational systems enforcing information integrity and confidentiality policies. Foundational issues associated with protection mechanisms [7] are presented. The identification of the security policy and its interpretation in terms of a technical policy for automated systems is covered. Informal and formal security policy models are addressed and both access-control and information flow models are reviewed [4][6].

The initial offering of a course on Security Policies, Models, and Formal Methods was given in the fall of 1996. Our Visiting Professor, William Shockley, was key to making this a successful effort. Offered as a class with three hours of lecture and a one hour laboratory session each week, students were guided through the theoretical underpinnings of computer security and were able to apply these concepts in a logical framework for proving system properties. The Stanford Research Institute Proof Verification System (PVS) was used to illustrate logical constructs in the laboratory.

4.2.5 Advanced Topics in Computer Security

This is a seminar course and is intended for advanced graduate students. Here we study the most recent papers and developments.

4.3 Student Theses

Master of Science theses have explored and are exploring diverse areas including: security policies, multilevel security, intrusion detection, issues associated with downgrading on automated systems, applications of cryptography, and web security.

Faculty research interests have a strong influence on thesis topic choices, however, should a student identify a valid topic outside of the usual areas, every effort is made to accommodate their research within the NPS CISR program.

5 Discussion

Computer security and INFOSEC cover a wide range of topics and requirements for personnel educated in these areas differ significantly between industry, academe, and the public sector [8][9]. NPS CISR is developing a comprehensive program in INFOSEC education and research that can become a resource for DoN/DoD and U.S Government in terms of educational materials and research. Building upon the foundations of computer science laid by the department's core curriculum, the security track conveys vital concepts and techniques associated with INFOSEC today. NPS CISR research programs permit students to conduct thesis work addressing DoD/DoN/U.S. Government concerns.

We are still in the early stages of the NPS CISR effort and much effort is still required to firmly establish our multi-faceted program and make it an ongoing success.

A major benefit of our program is the education of computer scientists and engineers whose understanding INFOSEC issues and potential problem solutions can contribute to the security of the information infrastructure.

References

1 Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D), Defense Science Board, Office of the Secretary of Defense, 3140 Defense Pentagon, Washington, DC 20301-3140, November 1996.

2 OPNAV INSTRUCTION 5239.X, Working Draft, 21 June 1996.

3 Anderson, James P, Computer Security Technology Planning Study, Air Force Electronic Systems Division, ESD-TR-73-51, Hanscom AFB, Bedford, MA, 1972. (Also available as Vol. I, DITCAD-758206. Vol. II, DITCAD-772806).

4 Bell, D. E., and LaPadula, L., Secure Computer Systems: Mathematical Foundations and Model, M74-244, MITRE Corp. Bedford, MA, 1973.

5 D. L. Brinkley and Schell, R. R., Concepts and Terminology for Computer Security, in Information Security: An Integrated Collection of Essays, ed. Abrams and Jajodia and Podell, IEEE Computer Society Press, Los Alamitos, CA, 1995, pp. 40-97.

6 Goguen, J. and Meseguer, J., Security Policies and Security Models, Proc. IEEE Symposium on Security and Privacy, Oakland, CA, IEEE Computer Society Press, Los Alamitos, CA, 1982, pp 11-20.

7 Harrison, M. and Ruzzo, W. and Ullman, J., Protection in Operating Systems, Comm. A. C. M., Vol. 19, No. 8, 1976, pp. 461-471.

8 Irvine, C.E., Goals for Computer Security Education, Proceedings of the IEEE Symposium on Security and Privacy, Oakland CA, IEEE Computer Society Press, Los Alamitos, CA, May 1996, pp. 24-25.

9 Irvine, C. E., Report on the First ACM Workshop on Education in Computer Security, SIG SAC Review, Vol. 15, No. 2, 1997, pp. 3-5.

10 Irvine, C.E., Warren, D. F., and Stemp, R., Teaching Introductory Computer Security at a Department of Defense University, NPSCS-97-002, April 1997.

11 Saltzer, J. H, and Michael D. Schroeder, M.D., The Protection of Information in Computer Systems, Proceedings of the IEEE, Vol. 63, No. 9, 1975, pp. 1278-1308.

12 Schell, Roger R., Computer Security: The Achilles' Heel of the Electronic Air Force, Air University Review, January-February, 1979, pp. 16-33.

..

Table 1. Naval Postgraduate School Center for INFOSEC Studies and Research
Computer Security Track

Quarter 1 (Fall or Spring)	Introductory Programming	Computing Devices and Systems	Logic and Discrete Mathematics	Intro. to Combinatorics & Its Applications	
Quarter 2 (Winter or Summer)	Advanced Programming	Data Structures	Introduction to Computer Architecture	Theory of Formal Languages and Automata	
Quarter 3 (Spring or Fall)	Programming in a Second Language	Theory of Algorithms	Introduction to Computer Security	Software Methodology	Research Seminar in Computer Science
Quarter 4 (Summer or Winter)	Artificial Intelligence	Database Systems	Operating Systems	Principles of Programming Languages	Thesis Planning Seminar
Quarter 5 (Fall or Spring)	Computer and Communications Networks	Computability Theory and Complexity	Secure Systems	Management of Secure Systems	
Quarter 6 (Winter or Summer)	Interactive Computation Systems	Thesis	Policies, Models and Formal Methods	Distributed Operating Systems	
Quarter 7 (Spring or Fall)	Joint & Maritime Strategic Planning	Thesis	Adv. Computer Security -- Database Security	Track Elective	
Quarter 8 (Summer or Winter)	Thesis	Thesis	App. Info. Sec. Systems -- Network Security	Advanced Topics in Computer Security	

1. Bold Outline indicates courses specifically required for the Computer Security Track
2. Advanced and Introductory Programming are in either Ada, Java, or C++
3. Data Structures requires students to use the language of their current Advanced Programming course
4. The second programming language is selected from Ada, Java, or C++
5. Joint and Maritime Strategic Planning is a course required of all Navy students. Students from the other services, U.S. Government, and allied nations often substitute other course work.