

**NAVAL POSTGRADUATE SCHOOL**  
**Monterey, California**



Teaching Introductory Computer Security  
at a  
Department of Defense University

by

Cynthia E. Irvine  
Roger Stemp  
Daniel F. Warren

April 1997

Approved for public release; distribution is unlimited.

Prepared for: Naval Postgraduate School  
Monterey, California 93943

NAVAL POSTGRADUATE SCHOOL  
Monterey, California

Rear Admiral M. J. Evans  
Superintendent

Richard Elster  
Provost

This report was prepared as part of the Naval Postgraduate School Center For Information Systems Security (INFOSEC) Studies and Research (NPS CISR) at the Naval Postgraduate School, which is currently funded by the National Security Agency under Contract No. H98230-R297-0030. Any opinions, findings, and conclusions or recommendations expressed in this report are those of the authors and do not necessarily reflect the views of the National Security Agency.

---

CYNTHIA E. IRVINE  
Assistant Professor  
Department of Computer Science

Reviewed by:

---

NEIL C. ROWE  
Associate Professor  
Department of Computer Science

Released by:

---

TED LEWIS  
Chairman  
Department of Computer Science

---

NETZER  
Dean of Research

# Teaching Introductory Computer Security at a Department of Defense University

Cynthia E. Irvine, Roger Stemp, and Daniel F. Warren

Naval Postgraduate School  
Department of Computer Science  
Monterey, California 93943-5118

April 1997

*Abstract*

*The Naval Postgraduate School Center for Information Systems Security (INFOSEC) Studies and Research (NPS CISR) has developed an instructional program in computer security. Its objective is to insure that students not only understand practical aspects of computer security associated with current technology, but also learn the fundamental principles that can be applied to the development of systems for which high confidence in policy enforcement can be achieved. Introduction to Computer Security, the cornerstone course for our program, is described here.*

## **1 Introduction**

Twenty-five years ago, computers were still largely monolithic mainframes, physically isolated from cyber-predators and closely tended by dedicated staffs of technical and administrative personnel. Even then, when computers were the domain of scientists and engineers, the need for computer security was recognized [22] and programs to achieve it pursued, e.g. [23].

Now society's relationship with the computer has changed dramatically. Computers are everywhere: in our tools and appliances, in our homes, schools and offices. They are used to manage our money and all phases of commercial enterprise. The evolution of techniques with which to download executable content either for work or entertainment from remote systems provides powerful mechanisms that tie together the far corners of the world as never before. Now computer security is no longer an esoteric subject discussed by a small group of academics and system administrators, but a topic that must be appreciated by all citizens of the information age. The education of computer security professionals is critical to the support of personal, corporate, and government information systems security objectives.

Over the past six years, at the Naval Postgraduate School (NPS), we have developed a 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). A cornerstone of the educational program offered by NPS CISR is the introductory course in computer security that we have developed. This report is intended to provide background regarding the rationale for the course's content and a detailed description of the course itself.

## **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. Thesis research allows students to be involved in work addressing an unsolved problem, usually within the framework of the U.S. Department of Defense (DoD) or U.S. Government; it enhances both their oral and written presentation skills, and it hones their critical thinking abilities. In many cases students start thesis research prior to the sixth quarter.

### **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. First, a two-course sequence in INFOSEC was offered: an introductory course and an advanced topics course. In 1994 the track was expanded and new INFOSEC courses were added to the Computer Science Curriculum.

With the encouragement of sponsors, the Naval Postgraduate School Center for INFOSEC Studies and Research 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 the following 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.

## **2.3 INFOSEC Curriculum**

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, and
- To enhance students' laboratory experience through the hands-on use of secure systems,
- To heighten awareness of security issues with non-computer science majors, such as those studying management or procurement.

### **2.3.1 NPS CISR Curriculum Philosophy**

To teach computer security, an accurate definition of the subject is needed. At the most general level, security pertains to access either to computational resources or to information in a computer system. Access to computational resources can be denied to legitimate users through the disruption of service, theft, or merely too little processing power or bandwidth for the amount of computation required. In contrast, information is vulnerable to unauthorized modification or disclosure. Access to information is controlled to prevent unauthorized modification and disclosure. Thus we have a triad of INFOSEC objectives:

- **Availability:** to ensure that information and/or resources are not being withheld in an unauthorized manner.
- **Confidentiality:** to ensure that information is not disclosed in an unauthorized manner.
- **Integrity:** to ensure that information is not modified in an unauthorized manner.

It is important to clearly separate problems in availability from those associated with confidentiality and integrity. For availability, we wish to ensure access to a resource, whereas, for

the other two, we wish to permit only authorized parties access to information. Students learn that availability is subjective, what is sufficient access to resources for one individual may be inadequate for another. Thus it is difficult to express an availability policy. In contrast confidentiality and integrity can be precisely defined and it is possible to know when a system has provided the necessary and sufficient mechanism to support either a confidentiality or an integrity policy, or both.

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 [4]. 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 requires systematic presentation of the principles of computer security and a corresponding engineering discipline. The feasibility of designing systems which are less susceptible to recurrent cycles of penetrations and patches [17] can be described and demonstrated.

In addition, our students must know how to function in the real world, where risk management techniques are employed [1]. 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.) Issues associated with the incremental achievement of security objectives must be addressed.

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.

## **2.4 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.

### 3 INFOSEC Curriculum

The INFOSEC courses for computer science students is integrated as a specialization track within the core computer science curriculum. The course matrix for the track is shown in Table 1.

**Table 1: Computer Security Track of NPS Computer Science Curriculum.**

<b>1st Quarter (Fall or Spring)</b>	CS-2970 (3-2) Object-Oriented Programming 1	CS-3010 (4-0) Computing Devices and Systems	MA-3025 (5-1) Logic and Discrete Mathematics	MA-3030 (5-1) Intro. to Combinatorics & Its Applications	
<b>2nd Quarter (Winter or Summer)</b>	CS-2972 (3-2) Object-Oriented Programming 2	CS-3300 (3-2) Data Structures	CS-3200 (3-2) Introduction to Computer Architecture	CS-3601 (4-0) Theory of Formal Languages & Automata	
<b>3rd Quarter (Spring or Fall)</b>	CS-3701 (3-2) Object-Oriented Programming in C++	CS-3650 (4-0) Theory of Algorithms	<b>CS-3600 (3-2) Introduction to Computer Security</b>	CS-3460 (3-1) Software Methodology	CS-4900 (2-0) Research Seminar in Computer Science
<b>4th Quarter (Summer or Winter)</b>	CS 3310 (4-0) Artificial Intelligence	CS 3320 (3-1) Database Systems	CS-3450 (3-2) Operating Systems	CS-3111 (4-0) Principles of Programming Languages	CS 4905
<b>5th Quarter (Fall or Spring)</b>	CS3502 (4-0) Computer and Communications Networks	<b>CS-3651(4-0) Computability Theory and Complexity</b>	CS-4600 (3-2) Secure Systems	CS-3670 (3-2) Management of Secure Systems	
<b>6th Quarter (Winter or Summer)</b>	CS 4203 (3-2) Interactive Computation Systems	Thesis	CS-4605 (3-1) Policies, Models and Formal Methods	CS-4112 (3-2) Distributed Operating Systems	
<b>7th Quarter (Spring or Fall)</b>	NS-3252 (4-0) Joint & Maritime Strategic Planning	Thesis	CS 4602 (4-0) Adv. Computer Security (Database Security)	Track Requirement	Note: International students replace NS-3252 with IT-1500.
<b>8th Quarter (Summer or Winter)</b>	Thesis	Thesis	CS-4614 (3-1) Advanced Topics in Computer Security	CS 3690 (4-0) App. Info. Sec. Systems (Network Security)	

**Bold Outline indicates courses specifically required for the Computer Security Track**

The track requirement in the seventh quarter is determined as appropriate based on the thesis research and interests of the individual student.

### 3.0.1 Introduction to Computer Security

Two courses, Introduction to Computer Security and Management of Secure Systems, provide an overview of INFOSEC principles and techniques described in section 2.3 . 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.

Introduction to Computer Security was the first course offered at NPS. 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. It included many of the topics now covered by the two current courses, Introduction to Computer Security and Management of Secure Systems. The original course skimmed many topics, but there was still insufficient time to survey all areas of computer security deemed important. Therefore, we decided to create two courses: one on the principles and underlying mechanisms for system security and the other on practical aspects of structuring and maintaining secure systems. In 1995, Introduction to Computer Security was modified to be an intermediate rather than an upper-level graduate course. 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 inclusion of extensive laboratory materials to accompany lectures. Although there were occasional demonstrations in class, the course was originally presented with no laboratory component. Now we have developed a set of laboratory exercises and tutorials which complement lecture material. Topics include: passwords, discretionary access controls, mandatory access controls, and use of Pretty Good Privacy (PGP). 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 Sun's Trusted Solaris and Wang Federal's XTS 300 system.

The course has been organized into eleven one-week units designed as a logical progression in INFOSEC principles. The prerequisites are: an introductory course on computer organization. It consists of three hours of lecture and two hours of laboratory work per week. We usually give three exams of equal weight during the course and collect approximately six homework and laboratory assignments. The catalog description is quoted here:

*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.*

With few books to choose from as texts, we elected to use a book that would give an overview of the field [15] and to provide an extensive set of other materials for assigned readings. Because the book had no homework problems, we had to devise all homework sets ourselves. Below is a brief outline of the topics covered in the NPS CISR version of Introduction to Computer Security. The references are to the supplementary reading assigned for each topic. One of the articles [7] is assigned over several weeks, because it covers a number of topics.

- Introduction to Computer Security- Definition, laws, historical perspective.
- Access Control I - Policies, Identification and Authentication, Discretionary Access Control [7]
- Access Control II - Mandatory Access Control and Supporting Policies [7]
- Building Secure Systems I - Design and Implementation concepts that support assurance [3]
- Malicious Software and Intrusion Detection - Trojan Horses, viruses, worms, detecting attacks. [9]
- Certification and Accreditation, Disaster Planning and Recovery, and Risk Analysis - certification and accreditation issues [2]
- Cryptography basics - private key, public key, and hashing schemes
- Cryptographic protocols - key management, voting, digital cash, secret sharing, one time password generation, Digital Signature Standard and Clipper. [10] [19] [21]
- Network Security - special considerations, combining access control and cryptography. [7]
- Network Security in Today's Environment - TCP/IP, Internet and firewalls [5] [8] [20]
- Building Secure Systems II - System evaluation issues [18] [13]

Like the subject it surveys, Introduction to Computer Security is dynamic. Each quarter we review the topics covered as well as the readings to ensure that they remain current and pertinent. We hope that this description of our course will encourage the interested reader to review the course notes which have been included as an appendix and to read some of the articles that we believe are useful supplements to the book.

## References

1. OPNAV INSTRUCTION 5239.X, Working Draft, 21 June 1996.
2. Issues in Quantitative versus Qualitative Risk Analysis, Datapro Reports on Information Security, IS20-250-101, McGraw-Hill, Delran, NJ, 1992.
3. Ames, S. H., Gasser, M. and Schell, R. R, Security Kernel Design and Implementation: An Introduction,IEEE Computer, Vol. 16, pp. 14-22, 1983.
4. 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)
5. Bagwill, R., Carnahan, L, Kuhn, R., Nakassis, A. Ransom, M., Barkley, J., Chang, S., Markovitz, P., Olsen, K., and Wack, J. Security in Open Systems, NIST Special Publication 800-7, ed. Barkley, Computer Systems Technology, U.S. Department of Commerce, National Institute of Standards and Technology.
6. Brinkley, D. L., and Schell, R. R., What Is There to Worry About? An Introduction to the Computer Security Problem, in Information Security: An Integrated Collection of Essays, ed. Abrams and Jajodia and Podell, IEEE Computer Society Press, Los Alamitos, CA, pp. 11-39, 1995.
7. Brinkley,D. L., 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, pp. 40-97, 1995.
8. Cheswick, W. R.. and Bellovin, S. M, An Evening with Berford In which a Cracker is Lured, Endured, and Studied, Chapter 10 in Firewalls and Internet Security, Addison Wesley, Reading, MA, 1994.
9. Denning, D., Neumann, P., and Parker, D., Social Aspects of Computer Security, in Proceedings 10th National Computer Security Conference, pp. 320-325, September 1987.
10. Denning, D., and Branstad, D., A Taxonomy for Key Escrow Encryption Systems, Comm. A.C.M., Vol 39, p. 34, 1996.
11. Fithen, K., and Fraser, B., CERT Incident Reponse and the Internet, Comm. A.C.M., Vol 37, pp. 108-133, 1994.
12. Landau, S., Kent, S., Brooks, C., Charney, S., Denning, D., Diffie, W., Lauck, A., Miller, D., Neumann, P., and Sobel, D., Crypto Policy Perspectives, Comm. A.C.M., Vol. 37, p. 115, 1994.
13. Lee, T. M. P., A Note on Compartmented Mode: To B2 or Not To B2?, in Proceedings 15th National Computer Security Conference, pp. 448-458, 1992.

14. Lunt, T. F., A Survey of Intrusion Detection Techniques, *Computer and Security*, Vol. 12, pp. 405-418, 1993.
15. Russell, D., and Gangemi, G. T., *Computer Security Basics*, O'Reilly & Associates, Inc., 1991.
16. Saltzer, J. H, and Michael D. Schroeder, M.D., The Protection of Information in Computer Systems, *Proceedings of the IEEE*, Vol. 63, No. 9, pp. 1278-1308, 1975.
17. Schell, Roger R., *Computer Security: The Achilles' Heel of the Electronic Air Force*, *Air University Review*, January-February, pp. 16-33, 1979.
18. Schell, R. R., and Brinkley, D. L., Evaluation Criteria for Trusted Systems, in *Information Security: An Integrated Collection of Essays*, ed. Abrams and Jajodia and Podell, IEEE Computer Society Press, Los Alamitos, CA, pp. 137-159, 1995.
19. Schneier, B., *Cryptography, Security, and the Future*, *Comm. A. C. M.*, Vol. 40, p. 138, 1997.
20. Wack, J.P. and Carnahan, L. J., *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*, NIST Special Publication 800-10, U.S. Department of Commerce, National Institute of Standards and Technology.
21. Walker, S.T., Lipner, S.B., Ellison, C.M., and Balenson, D.M., *Commercial Key Recovery*, *Comm. A.C.M.*, Vol. 39, p. 41, 1996.
22. Ware, W., *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security*. Rand Corporation, 1970. AD-A076617/0.
23. Weissman, C., *Security Controls in the ADEPT-50 Time Sharing System*. In *Proceedings of the 1069 AFIPS Fall Joint Computer Conference*, pp. 119-133. AFIPS Press, 1969.