NAVAL POSTGRADUATE SCHOOLCENTER FOR INFOSEC STUDIES AND RESEARCH: TEACHING THE SCIENCE OF COMPUTER SECURITY (U)

Cynthia E. Irvine

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

(U) ABSTRACT

(U) 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 has been established. Its philosophical core is the abstract notion of conceptually complete security mechanism, the Reference Monitor Concept. Building upon a core curriculum of computer science and engineering, the security courses convey vital concepts and techniques associated with INFOSEC today.

(U) INTRODUCTION

(U) 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 and programs to achieve it were pursued [13]. Today, code is moved across the vast reaches of the World Wide Web and ad hoc networks are created from commercial products, many having questionable security properties.

(U) In response to a growing concern regarding the vulnerability of the National Information Infrastructure, a 1996 Defense Science Board [1] study cited the need for broader and deeper education in the building of resilient systems. In particular, the task force noted that to address the challenge of information warfare-protect (IW-P), a cadre of computer scientists with M.S. 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.

(U) The Naval Postgraduate School a(NPS) anticipated this recommendation by five years. Starting in the early 1990s, the Computer Science Department at NPS has developed a program in INFOSEC and in 1996 established the Naval Postgraduate School Center for INFOSEC Studies and Research (NPS CISR). Today, NPS CISR involves the research of eight faculty and staff members, nine thesis students, and approximately 150 students from the Computer Science, Information Technology Management and Information Warfare curricula participating in classes and laboratory work annually.

(U) NPS CISR is serving as a model program which can be emulated by both DoD and civilian universities. It addresses the INFOSEC research and education needs of DoD and U.S. Government in the following major areas.

- (U) Curriculum development ensures that a coherent and comprehensive program in INFOSEC foundations and technology is presented at the university and postgraduate levels.
- (U) Development of the INFOSEC and Trusted Systems Laboratory supports the INFOSEC teaching and research programs at NPS.
- (U) 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.
- (U) A Visiting Professor program which brings INFOSEC experts to NPS to offer courses and engage in research with faculty and students.
- (U) An Invited Lecture series injects commercial and military relevance into the NPS CISR activities.
- (U) An academic outreach program permits other, non-CISR academic institutions to benefit from the INFOSEC education and research developments at NPS.

Appeared in Proceedings of MILCOM 97, (Unclassified), Monterey, CA, Vol 1, pp. 405-409, November 1997.

- (U) 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.
- (U) Research, focusing on INFOSEC problems, with emphasis on those of DoN, DoD, and U.S. Government.

(U) This paper will provide a synopsis of the NPS CISR curriculum with motivation for its philosophical approach.

(U) COMPUTER SCIENCE AT NPS

(U) The educational program at NPS CISR is based upon the recognition that INFOSEC solutions must be designed, implemented and managed by individuals who understand which solutions work and which are merely speculation and hyperbole. A solid grounding in the principles of computer science combined with INFOSEC specialization courses prepares graduates to tackle current and future INFOSEC challenges.

(U) The Computer Security option is a specialization area within the two-year, eight-quarter Masters degree program at the Naval Postgraduate School. A rigorous core curriculum of traditional computer science offered in the first year is required of all students and prepares them for the any of an number of specialty tracks. Courses 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.

(U) 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 option. Often motivated students start students well in advance of the official sixth quarter start time. Since faculty research is generally centered on topics of interest to DoD and U.S. Government, student thesis research accrues many benefits beyond creative thinking, analysis, and development of presentation skills.

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

- (U) To provide both introductory and advanced courses,
- (U) To provide courses accessible by students who are not in the Computer Science curriculum, including those studying management or acquisition
- (U) To insure that Computer Science students have a strong foundation upon which to base advanced course work in computer science and INFOSEC,
- (U) To involve students in ongoing computer security and INFOSEC research and technology development,
- (U) To enhance students' laboratory experience through practical experience in the use of secure systems, and

(U) SECURITY PHILOSOPHY AND BALANCE

(U) A serious problem facing educators addressing computer security and IW-P is balancing the need to equip graduates with knowledge and facility in the use of current tools and technologies to address immediate security threats, against the goal of education in the fundamental principles of computer security required for the development of practical and effective security solutions for both near-term and long-range systems. In the NPS CISR curriculum, we integrate current tools and technologies experience into a rigorous program based on foundational concepts in computer security.

(U) The fundamental security idea that provides the foundation for the entire NPS CISR curriculum is 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 [7] 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].

(U) REFERENCE MONITOR EXAMPLE

(U) In any system it is assumed that there are active entities, in computer security parlance they are called subjects, and passive entities, called objects. The Reference Monitor Concept articulates the abstract notion that there can be a mechanism to mediate the accesses of subjects to objects. It encompasses three properties:

- (U) It is tamperproof
- (U) It is always invoked
- (U) It is small enough so that it can be analyzed for completeness and correctness.

(U) A simple example of failure to implement an instance of the Reference Monitor Concept illustrates why it is central to any sound security architecture.

(U) Hypothesize a PCMCIA card (*smart card*) issued by "Seashore Bank"[1]. Programmed by the bank, the card encapsulates the keys and algorithms required for the use of

various cryptographic protocols. Assume that the card is tamperproof. (It is known that given sufficient work, the card may not be not be tamperproof, but it is "good enough." [4]) Each user is also provided with card driver software and application software for a number of banking functions. We assume that the smart cards plug into a PCMCIA device port [5].

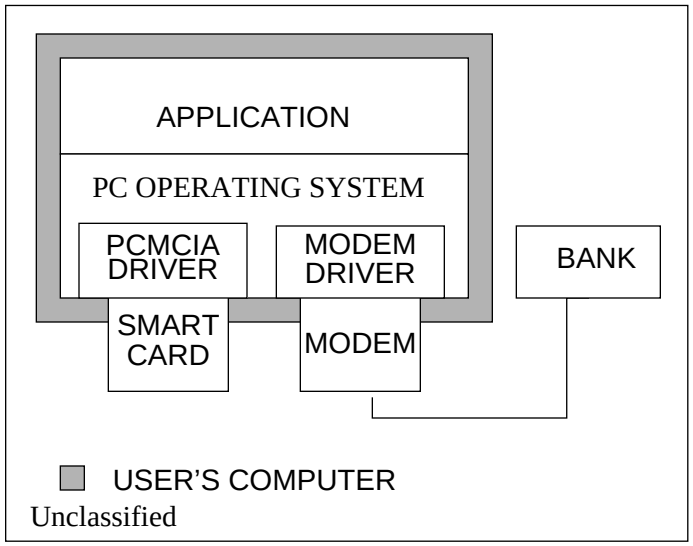

Figure 1: (U) Hypothetical PC for Banking Applications

(U) The system architecture shown in Figure 1. Of particular note is the independence of the smart card and the modem.

(U) The customer assumes that transactions with the bank are protected by the use of the cryptography available in the smart card. For example, if the customer wishes to send some personal information to the bank, it will be encrypted to protect the confidentiality of the information. Unfortunately our unsuspecting user does not know that the Reference Monitor Concept was not considered in the system design, so many things can go wrong.

(U) Our user happens to be an inveterate World Wide Web aficionado and when visiting a "cool" site, downloaded a fancy multi media package. Unknown to the user, this package contained a clandestine artifice so that when it was executed, a few unexpected things happened. It exploited a flaw in the operating system to implant new code to service banking requests. Now, instead of encrypting the user's personal information by calling the smart card for encryption services nothing is done. (An alternative would be to apply a trivial cipher to the data.) User information is sent to the modem unencrypted. The smart card's encryption services have been bypassed.

1. (U) This name is intended to be fictitious.

(U) There are endless variations on this scenario including modifications to the application, exploitation of various operating system flaws, subversion of the driver, and so on. In all cases, the outcome is the same: there was no way to be certain that the encryption protocol is being followed.

(U) Identification and repair of the operating system flaw that allowed the attack, is only a temporary fix until another flaw is identified and exploited. The malicious multi media package may be frequently updated by its mischievous developers, so that although a user system may contain patches to the known vulnerabilities exploited by the malicious software, other vulnerabilities are still available for attack. It would be impossible to enumerate all of the possible ways that the system could be exploited.

(U) Thus the user community and the bad guys end up in a game of "penetrate and patch." The good guys have to plug up all of the possible holes in their system while the bad guys need only find one vulnerability in order to launch a successful attack.

(U) How could this happen? How could it be prevented? The user expected the smart card to be "always invoked," but it hasn't been. Why? Because the smart card is part of a larger system that includes drivers, operating system, and application-level software. The smart card may do its encryption job very well, but if there is no reliable way to ensure that it will be used correctly and for every transmission to the bank, then, in terms of security, the system is incomplete. Secure system design principles require that protection critical components are always used and are protected from tampering. Had this been done, the user's personal information would have been safe. For example, had the operating system been designed so that it was self protecting, then malicious application-level software would be unable to change it.

(U) A simple redesign is illustrated in Figure 2. It is not a complete security solution (you need to take our classes to have the entire picture), but provides an example of one aspect of a good security engineering design. Here it is impossible to use the modem to send information to the bank without invoking the smart card. Thus there is assurance that the information flows through the smart card.

(U) Unlike many other things in this world, computers are designed to do what they are told to do. Hence if a computer is designed to limit access to critical programs and information to only those authorized to read and/or modify it, then it will always follow those instructions. (Admittedly, this is easier said than done, but it is a notion based on the idea that computers are built to perform the same task consistently: that at the lowest level bits are either set to zero or one, on or off, yes or no, grant access or deny access.)

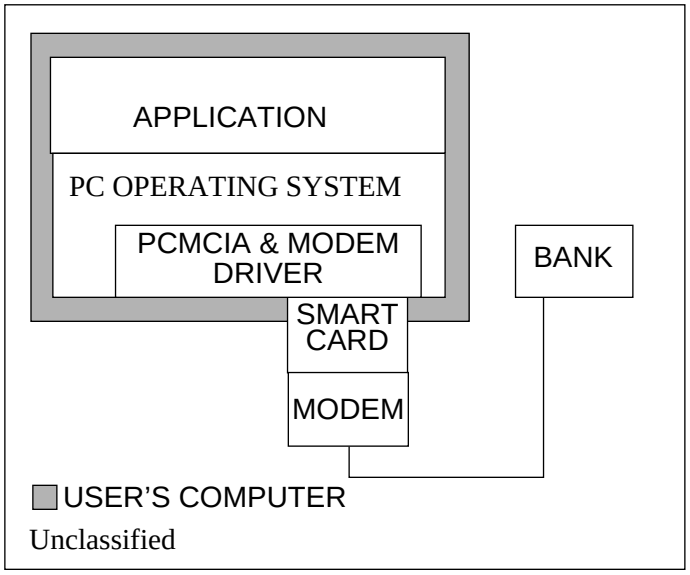

Figure 2: (U) Improved Hypothetical PC for Banking Applications

(U) NPS CISR COURSES

(U) Our emphasis on the Reference Monitor Concept is tempered with course work intended to provide a perspective on the many areas that contribute to computer security. By creating a coherent sequence of 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 case studies, students understand how past problems have been solved and have an opportunity to consider current topics.

(U) Advanced courses 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 hardware security in greater depth.

(U) The ultimate objective of all INFOSEC studies is to improve security in real systems. Thus, practical laboratory experience is crucial to an effective INFOSEC program. Laboratory exercises including tutorials and projects reinforce and extend concepts conveyed in lectures and prepare students for effective thesis research. Students use 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.

(U) Two courses, Introduction to Computer Security and Management of Secure Systems, complement each other and provide a survey of INFOSEC principles and techniques. They review both the conceptually complete and more intuitive approaches to INFOSEC providing students with an appreciation of both foundational concepts and current practice in computer security.

(U) By design, **Introduction to Computer Security** may be taken by science and engineering students early during their tenure at NPS. Benefits are: a larger number of DoD personnel with a broad overview of INFOSEC issues; early sensitization to key principles in computer security leading to an appreciation of the interplay of security with other aspects of computer and distributed systems science and engineering. Our position as a DoD university is reflected in some course units, however, most or the topics covered are universal. They include: 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 included as needed. Broad rather than deep, the course provides the basis for advanced security studies.

(U) **Management of Secure Systems** complements Introduction to Computer Security and includes lectures and extensive laboratory and field exercises covering risk analysis, certification and accreditation, system maintenance tools, and organizational aspects of INFOSEC, with particular focus on military systems [2].

(U) **Network Security** for both open systems and military 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.

(U) **Database Security** is being developed to include not only traditional database security, but issues associated with workflow and transaction processing.

(U) **Secure Systems** 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 learn how software engineering principles such as modularity and layering, minimization, configuration management, and the fault hypothesis method can be used to build secure and resilient systems.

(U) **Security 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 [9] 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 for access-control and information flow are reviewed [6][8]. Laboratory work helps students master the theoretical underpinnings of computer security and apply these concepts in a logical framework for proving system properties, i.e., the Stanford Research Institute Proof Verification System (PVS) [10].

(U) **Advanced Topics in Computer Security** is a seminar course and is intended for advanced graduate students. Here we study the most recent papers and developments.

(U) **Thesis Research** 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.

(U) Faculty research interests influence 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.

(U) CONCLUSION

(U) 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.

(U) The NPS CISR program is still young and substantial effort is still required to firmly establish our multi-faceted program and make it an ongoing success.

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

(U) REFERENCES

1 (U) 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, Nov. 1996.

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

3 (U) Anderson, J. 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 (U) Anderson, R., and Kuhn, M., Tamper Resistance - A Cautionary Note, *Proceedings of the 2nd Workshop on Electronic Commerce*, Oakland, CA, 1996

5 (U) Beatty, D. L, Kipisz, S., M, and Moore, B. E., The PCMCIA Software Developer's Handbook, Peer-to-Peer Communications, 1996.

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

7 (U) 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, pp 40-97, 1995.

8 (U) Goguen, J. and Meseguer, J., Security Policies and Security Models, *Proc. IEEE Symposium on Security and Privacy, Oakland*, CA, Computer Society press, pp 11-20, 1982.

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

10 (U) Rushby, J. Stringer-Calvert, D. W. J., A Less Elementary Tutorial for the PVS Specification and Verification Language, SRI Technical Report, CSL-95-10, SRI International, Menlo Park, CA 1996.

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

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

13 (U) Schroeder, M.l D.,Clark, D., and Saltzer, J., The Multics Kernel Design Project, *Proceedings of Sixth A.C.M. Symposium on Operating System Principles*, pp. 43-56, 1977.