1997-12

An information security education initiative for engineering and computer science

Chin, Shiu-Kai; Irvine, Cynthia E.; Frincke, Deborah

Monterey, California. Naval Postgraduate School

NPS-CS-97-003

NAVAL POSTGRADUATE SCHOOL
Monterey, California

An Information Security Education Initiative for Engineering and Computer Science

by

Shiu-Kai Chin
Cynthia E. Irvine
Deborah Frincke

December 1997

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:

DANBOGER
Acting Dean of Division of Computer and Operations

DAVID NETZER
Dean of Research

REPORT DOCUMENTATION PAGE

Form **approved**
OMB No **0704-0188**

1. AGENCY USE ONLY (Leave blank)	2. REPORTDATE	3. REPORT TYPE AND DATES COVERED
	1997 December 1	Progress; 10/1/97 - 12/1/97

An Information Security Education Initiative for Engineering and Computer Science

HR98230-R2-98-8004

6. AUTHOR(S)
Shiu-Kai Chin, Cynthia E. Irvine, and Deborah Frinke

7. PERFORMING ORGANIZATIONNAME(S) ***AND*** ADDRESS(ES)
Naval Postgraduate School, Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER
NPSCS-97 -003

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS —)
National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release;
Distribution is unlimited

12b. DISTRIBUTION CODE

14. SUBJECTTERMS
computer security, INFOSEC, education, engineering, assessment

15. NUMBER OF PAGES 27

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OFABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	Unlimited

NSN 7540-01-280-5800

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std 239-18

Enclosure (6)

An Information Security Education Initiative for Engineering and Computer Science

Shiu-Kai Chin
Department of Electrical and Computer Engineering
Syracuse University
Syracuse, NY **13224**

Cynthia Irvine
Center for INFOSEC Studies and Research
Naval Postgraduate School
Monterey, CA **93943**

Deborah Frincke
Department of Computer Science
University of Idaho
Moscow, ID **83844**

Abstract

This paper puts forward a case for an educational initiative in information security at both the undergraduate and graduate levels. Its focus is on the need for such education, the desired educational outcomes, and how the outcomes may be assessed. **A** basic thesis of this paper is that the goals, methods, and evaluation techniques of information and computer security are consistent with and supportive of the stated goals of engineering education and the growing movement for outcomes-based assessment in higher education.

1 Why Information Security Education is Needed

Networked computing and information retrieval are considered by many to be crucial to the well-being of the nation's information infrastructure [14]. The information infrastructure includes such diverse and complex applications as telecommunications, air traffic control, health care, mobile computing and electronic commerce. These applications rely on a collection of switching systems, databases, network protocols, scheduling and routing algorithms, distributed hardware, and concurrent software. These systems must work correctly and economically with guarantees of performance, availability of service, safety, and security.

The increasing use, reliance upon, and vulnerability of these large-scale information systems is called the "Information Security Problem" by the National Research Council in its book, *Cryptography's Role in Securing the Information Society*, [40].

> Today's information age requires U.S. businesses to compete on a worldwide basis, sharing sensitive information with appropriate parties while protecting that information against competitors, vandals, suppliers, customers, and foreign governments. Private law-abiding citizens dislike the ease with which personal telephone calls can be tapped, especially those carried on cellular or cordless telephones. Elements of the U.S. civilian infrastructure such **as** the banking system, the electric power grid, the public switched telecommunications network, and the air traffic control

system are central to so many dimensions of modern life that protecting these elements must have a high priority.

One of the major problems confronting the security community cited by Pfleeger and Cooper [29] is: *"The advances in computer security have not been able to keep pace with the changes in computing in general."* In the rush to field new products and services, developers have often ignored security as a fundamental system requirement.

The Defense Science Board puts it more bluntly in its November 1996 report, *Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D)* [7]:

> The reality is that the vulnerability of the Department of Defense – and of the nation – to offensive information warfare attack is largely a self-created problem. Program by program, economic sector by economic sector, we have based critical functions on inadequately protected telecomputing services. In aggregate, we have created a target-rich environment and the U.S. industry has sold globally much of the generic technology that can be used to strike these targets.

The challenge is to design, develop and deploy complex systems with confidence in their ability to satisfy security requirements. Fortunately, a "Theory of Computer Security" [8] has emerged that has three components: a precisely articulated security policy describing the mangement, protection, and distribution of sensitive information by an organization, a set of functional mechanisms sufficient to enforce the policy, and assurance that the mechanisms do enforce the policy. Its implications are that:

- to achieve a coherent security architecture, security must be considered from the outset and not as an afterthought; and
- competence in design for security policy enforcement, testing for security, and assessment of security must be part of the education of system implementors.

Currently, few resources are being applied to educating security professionals, as noted by Spafford [42]:

> Our students and soon-to-be students will be designing our information technologies of the future. We are endangering them and ourselves because the majority of them will receive no training in information security.

Executive Order 13010 established a Presidential Commission on Critical Infrastructure Protection [27]. Strategies for security against computer-based attacks on information and computer systems are a primary commission objective and "education on methods of reducing vulnerabilities and responding to attacks on critical infrastructures" is an concern. To remedy the lack of computer science professionals educated in computer security noted by Spafford [42], the Commission has recommended [28] significant efforts to foster programs producing graduates in information and computer security.

The above need for education is echoed by the Defense Science Board. It recommends:

- working with the National Science Foundation to *"develop educational programs for curriculum development at the undergraduate and graduate levels in resilient system design practices,"* and

- making the *((requiredskill set much broader and deeper in educational level [for] computer scientists, network engineers, electronics engineers, business process engineers."*

To satisfy the above educational goals we must move to a *culture* of *engineering.* Broadly speaking, engineering is fundamentally about *assuring results* using techniques based on *scientific principles.* The goal is to *engineer* secure systems *ab initio* with assurance rather than to *discover* that what we have built is inadequate. Do current engineering and computer science curricula provide students with an understanding of the foundational concepts of computer security? The answer is "no." Computer security differs from other engineering approaches in that the system must be implemented such that security policy enforcement takes place *even in the presence* of *malicious code.* At the **1996** IEEE Symposium on Security and Privacy, Schell [39] noted that in the context of a subverted system a lack of security may not be evident.

By moving to a culture of engineering which includes appropriate knowledge of security, we can increase the likelihood that our next generation of information technology workers will have the background they need to design and develop systems which are engineered to be reliable and secure – that they are designed to protect information in the face of malicious software [8].

The security community has long embraced the concepts of requirements, policies, specifications, application of best implementation practices, assessment, and certification. When looking at curriculum development, analogous notions hold. These educational notions include:

- identification of educational criteria for selection of educational outcomes;
- identification of specific educational outcomes and skills;
- design of courses and curricula to meet the identified outcomes;
- designing means of assessment to evaluate the satisfaction of outcomes;
- assessing the actual outcomes; and
- utilizing feedback from assessment to improve curricula and courses.

The technique of identifying specific educational goals, assessing the results, and using these assessment results to improve educational processes is fully embraced by both the Accreditation Board for Engineering and Technology (ABET) for accrediting ***all*** engineering programs in the US [12], and by the American Society for Engineering Education (ASEE), [13]. Examining the educational goals of information security within the context of engineering and ABET accreditation is appropriate. Electrical and computer engineers, and computer scientists, many of whom are educated within colleges of engineering, are responsible for the design, implementation, and deployment of much of the information infrastructure. Their knowledge and understanding of the principles underlying and the engineering techniques used to construct secure systems is essential for the protection of systems from the smallest to the largest and at **all** levels of civilian and government enterprise. This paper provides a framework for integrating information security into computer science and computer engineering education.

The remainder of this paper is organized as follows. Section 2 discusses the criteria used to select the educational outcomes in Section **3.** Section **3** relates the educational goals of security and engineering and computer science within a common framework. Section **4** outlines proposed assessment criteria. Section 5 discusses computer security education programs. Conclusions are in Section 6.

2 Criteria for Selecting Educational Outcomes

It is insufficient and impractical to say everybody needs to know everything about security. Knowledge and skills appropriate to each role in the "information society" must be identified. There is a need for technical literacy among decision makers within enterprises, government, military defense, health care, higher education, etc. The focus here is on technical education in computer and network security. The overarching criteria for selecting educational outcomes for information security are:

- the educational outcomes must address security needs consistent with the security challenges encountered by graduates in their professional roles, and
- the specific educational outcomes for security in a given educational program must be consistent with the educational context and larger outcomes of the specific program.

Irvine in "Challenges in Computer Security Education," [20], identifies ten roles or job titles with associated security concerns. These roles are:

1. the general population;
2. corporate information professionals;
3. computer professionals;
4. system administrators;
5. computer security emergency response team (CERT) members;
6. secure software and hardware developers;
7. system architects;
8. system certifiers;
9. legal professionals and law enforcement; and
10. security researchers.

Of the above ten roles, programs of electrical and computer engineering and computer science are primarily concerned with the education of *software and hardware developers, system architects, system certifiers, CERT members,* and *security researchers.* For these roles, Irvine [20] identifies educational needs for each as follows:

- *Software and hardware developers,* when developing new components, should know how to build security into products. They should understand how hardware can support security objectives and how software can leverage hardware to produce systems able to enforce specific security policies.

- *System architects* must know how different security mechanisms within the system work together; a flawed component can obviate all other protection features. They must understand overall requirements and must be able to design a system that meets a variety of obligations, including those of security.

- *System certifiers* must know how to inspect the design and implementation of systems to determine the level of confidence to be ascribed to those systems' ability to enforce security policies. They must understand the properties of the underlying hardware as well as the software and must be able to analyze the evidence that high level policy is mapped to the policy enforcement mechanism. Rigorous approaches to flaw analysis and the exposure of system elements vulnerable to clandestine exploitation are required.

- *CERT members* must know how flaws in existing systems make those systems vulnerable to external threats. They must understand both hardware and software factors that contribute to the creation of system flaws and vulnerabilities, and generalize solutions across potentially large sets of services and products.

- *Security researchers* push the technological envelope. They must understand the interplay between security and other system properties such as fault tolerance and real-time constraints. They should have a deep understanding of computer science and the scientific foundations of computer security, and have significant specialized knowledge in their area of research.

How well do these goals match with the evaluation criteria for engineering and computer science programs? The Computing Sciences Accreditation Board (CSAB) criteria for curriculum assessment emphasizes the importance of the scientific method as a key concept within a computer science curriculum [9]. Table 1 below lists the skill set specified by ABET in its report, *Engineering Criteria 2000* [12].

Comparing the security skills needed by 1) software and hardware developers, 2) system architects, 3) system certifiers, 4) CERT members and 5) researchers, with the ABET criteria reveals a close match in the following areas:

- an ability to apply knowledge of mathematics, science, and engineering;

- an ability to design and conduct experiments, as well as to analyze and interpret data;

- an ability to design a system, component, or process to meet desired needs;

- an ability to identify, formulate, and solve engineering problems

- an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice; and

- an ability to communicate effectively.

Additionally, the broader areas of

- an understanding of professional and ethical responsibility;

- the broad education necessary to understand the impact of engineering solutions in a global and societal context; and

Table 1: ABET Evaluation Criteria for Engineering Programs

Criterion **3. Program Outcomes and Assessment**
Engineering programs must demonstrate that their graduates have
1. an ability to apply knowledge of mathematics, science, and engineering
2. an ability to design and conduct experiments, **as** well **as** to analyze and interpret data
3. an ability to design a system, component, or process to meet desired needs
4. an ability to function on multi-disciplinary team (CERT) members
5. an ability to identify, formulate, and solve engineering problems
6. an understanding of professional and ethical responsibility
7. an ability to communicate effectively
8. the broad education necessary to understand the impact of engineering solutions in a global and societal context
9. a recognition of the need for, and an ability to engage in life-long learning
10. a knowledge **of** contemporary issues
11. an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.

- a knowledge of contemporary issues

provide meaningful connections to the other roles identified by Irvine in [20].

Section **3** refines the connections between security and engineering education goals within a common framework.

3 Educational Outcomes

In Section **2** we juxtaposed the educational goals of engineering and computer science against the educational needs in the area of security for various societal roles. In this section we will relate the two in more detail so that the educational goals of security for hardware and software developers, system architects, system certifiers, CERT members, and potential researchers are met within the framework of engineering and computer science programs. To do so, we will examine the goals of each within a common framework of *critical thinking* which is applied across virtually all university disciplines.

Why examine both goals within a framework of critical thinking? First, the disciplines of security, engineering, and computer science are concerned with *solving problems* in their respective fields of interest. Second, each field has *systematic ways* of *thinking* and analysis for arriving at solutions. Third, each field has *standards.* Fourth, each field has notions of *evaluation and assessment.* Finally, working within a common framework shared by many other disciplines allows us to relate goals for security education to broader educational objectives and allows us to adapt assessment techniques used by other disciplines to security as science and engineering.

In Section **3.1** we describe a framework for critical thinking. Section **3.2** relates the disciplines of security, engineering, and computer science within that framework. Section **3.3** examines how

well the relationship between security and engineering meets the educational goals of information security and engineering on the basis of published criteria and goals.

3.1 A Framework for Critical Thinking

The importance of critical thinking as a higher order framework is identified by former Secretary of Labor, Robert Reich in his book, *The Work of Nations*, [31]. Reich puts forth four skills in particular: **1)** abstraction, **2)** system thinking, **3)** experimentation and testing, and **4)** collaboration. Paul and Willsen in [33] summarize Reich's list of skills as follows:

1. **Command of Abstractions**

   > The capacity for abstraction – for discovering patterns and meanings – is, of course, the very essence of symbolic analysis, in which reality must be simplified so that it can be understood and manipulated in new ways ... (pp. **229 – 230)**

2. **Thinking Within Systems**

   > The education of the symbolic analyst emphasizes system thinking. Rather than teach students how to solve a problem that is presented to them, they are taught to examine why the problem arises and how it is connected to other problems. (p. **231)**

3. **Testing Ideas**

   > Instead of emphasizing the transmission of information, the focus is on judgment and interpretation. The student is taught to get ***behind*** the data – to ask why certain facts have been selected, why they are important, how they were deduced, and how they might be contradicted. The student learns to examine reality from many angles, in different lights, and thus to visualize new possibilities and choices. The symbolic-analytic mind is trained to be skeptical, curious, and creative. (p. **230)**

4. **Learning to Collaborate and Communicate**

   > Students learn to articulate, clarify, and then restate for one another how they identify and find answers. They learn how to seek and accept criticism from peers, solicit help, and give credit to others. They also learn to negotiate – to explain their own needs, to discern what others need and view things from others' perspectives. (p. **233)**

The list of skills identified by Reich is the essence of critical thinking. Critical thinking is described by Diane Halpern [17] as:

> the use of those cognitive skills or strategies that increase the probability of a desirable outcome. It is ... purposeful, reasoned, and goal directed – the kind of thinking involved in solving problems, formulating inferences, calculating likelihoods, and making decisions when the thinker is using skills that are thoughtful and effective for the particular context and type of thinking task.

Richard Paul and Jane Willsen in [34] refine Halpern's definition to an individual's point of view as a series of questions:

What is the *purpose* of my thinking?
What precise *question* am I trying to answer?
Within what *point of view* am I thinking?
What *information* am I using?
How am I *interpreting* that information?
What *concepts* or ideas are central to my thinking?
What *conclusions* am I coming to?
What am I taking for granted, what *assumptions* am I making?
If I accept the conclusions, what are the *implications?*
What would the *consequences* be, if I put my thought into action?

The framework we use to describe security and engineering is based on the critical thinking framework of Paul and Nosich, [32]:

1. What is the discipline's purpose, goal, or end?
2. What are the questions at issue, or problems to be solved?
3. What are the discipline's points of view, or frames of reference?
4. What are the empirical dimensions of reasoning in the discipline?
5. What are the conceptual dimensions of reasoning?
6. What assumptions are made by the discipline?
7. How is the discipline used to draw implications and consequences?
8. What inferences can be made drawing upon the discipline?

Using the above framework, we can answer the questions as they pertain to security and engineering, and relate the two disciplines within the framework.

3.2 Relating Security, Engineering, and Computer Science Within a Framework of Critical Thinking

In *Goals for Security Education* [19] and *NPS CISR: Six Years of Experience* [21], Irvine describes topics chosen to illustrate and enforce the notion [4] that certain components of the system must be designed to be both continuously effective in enforcing policy and resistant to malicious software:

- security policy models
- formal methods applied to system specification, development, and analysis
- hardware and software protection mechanisms
- secure system design, implementation and testing
- database security
- modern cryptography
- cryptographic protocols
- key management and key distribution
- auditing
- identification and authentication
- coherent network security architectures

Pfleeger and Cooper in [29] list five broad classifications of security concepts.

1. *Policy* – understanding threats from which information requires protection to insure confidentiality, integrity, and availability.
2. *Privilege* – creating mechanisms to distinguish and control the ability **of** active system entities to access and affect system resources.
3. *Identification and authorization* – associating the activities of the executing computer with individual users, who may be held accountable for the activities undertaken on their behalf.
4. *Correctness* – with providing assurance that the hardware, software, and systems for security policy enforcement are not susceptible to tampering or bypass.
5. *Audit* – the creation of traces and their interpretation.

The above are a mixture of techniques, goals, and properties. To relate them to computer engineering and science curricula, we use the framework as shown in Table **2.** Sections **3.2.1** through **3.2.8** summarize the elements of each discipline within the framework. Educational outcomes are listed for each element.

3.2.1 Purpose, Goal, or End

Major goals in computer engineering and computer science is to construct computer systems or processes which meet a desired end or requirement. **A** major goal of security is to develop computing systems that can ensure security policy enforcement in the presence of malicious software and abusive user behavior. Hence the goal may encompass policy objectives for information confidentiality, integrity, and availability. In addition, the system must provide a mechanism to hold its

Table 2: Security and Engineering in a Critical Framework

Elements	*Security*	*Engineering*
Purpose, goal, or end.	Develop security policy based on threats. Build system providing assurance of correct and continuous security policy enforcement.	Construct computer systems or processes to meet a desired end or requirement.
Questions or problems to be solved.	How are security properties described in the context of an automated system? How are security properties engineered into systems? What assurance can be provided that these properties do in fact exist in the implementation and that they are tamper-resistant?	What are the structures of hardware, software, and subsystem components which satisfy the properties? What is the means of construction? By what means are the design and implementation verified and tested?
Points of view and frames of reference.	Architects, software designers, hardware designers. Various applications: operating systems, secure subsystems, secure networking and distributed computing, databases, etc.	Architects, software designers, hardware designers. Various applications: processors, operating systems, compilers, databases, etc.
Empirical dimensions of reasoning.	Experiments. Penetration testing, flaw hypothesis methodology, covert channel analysis, laboratory demonstrations, system administration issues, problems in commercial systems.	Experiments. Laboratory demonstrations, prototypes, simulation, testing, performance measurements.
Conceptual dimensions of reasoning.	Principles of construction and analysis. Information theory, discrete mathematics, cryptography theory, formal protocols, formal logics, formal methods, object-model design.	Principles of construction and analysis. Switching theory, finite automata, discrete mathematics, linear systems theory, logic, declarative programming, object-oriented design.
Assumptions made.	Components, services, functions, and properties for each level of design and frame of reference.	Components, services, functions, and properties for each level of design and frame of reference.
Implications and consequences.	Risk analysis. Maintenance. User acceptability. Trusted distribution. Configuration management. Cost. Ethics.	Risk, safety, and reliability analysis. Ease of manufacture. Cost. Ease of maintenance. Ethics.
Inferences.	Auditing and trace analysis. Intrusion detection. Fail secure operation. System test and verification.	Fault detection. Error detection. System test and verification.

users accountable for their actions through identification and authentication, and audit. Finally, users must have confidence that their information will, in fact, be protected within the system.

Educational Outcomes

- Ability to clearly state the purpose of a requirement, its significance, and its achievability.
- Ability to determine the consistency of requirements and purposes.

3.2.2 Questions or Problems to be Solved

The fundamental characteristic of engineering is the ability to answer the question, *does this structure* of *components have the properties which are required?* This question is asked at **all** levels of design, from the level where components are transistors, to the level where components themselves are systems of hardware and software.

In system design, many properties must be satisfied. Security requirements, broken down to confidentiality, integrity, and availability, are formulated as properties that must hold during system operation. The question at each level of design is, *does this structure* of *components map to a mechanism* ***for*** *security policy enforcement* ***for*** *which we have confidence in the presence* of *malicious code?* The use of formal security policy models, formal specifications, and assurance mappings to provide a chain of evidence that the implementation does correspond to policy, in combination with the development of high level security architectures and their step-wise refinement permits the precise articulation of security requirements and demonstrates the feasibility of a real implementation.

Educational Outcomes

- Ability to clearly formulate questions of significance relative to the overall purpose.
- Ability to clearly and precisely state the problem to be solved and how it can be decomposed.
- Ability to determine feasibility of problem solution.

3.2.3 Points of View and Frames of Reference

The points of view and frames of reference for both security and engineering are given in terms of roles and applications. The technical roles in security were identified in Section 2 as system architects, software and hardware developers, system certifiers, CERT members, and hardware designers. These roles have meaning in both engineering and security. These roles are characterized mainly by the components, functions, services, and means of reasoning available to each.

For example, system architects assume as components particular networks, network services, hardware platforms, and operating systems. Security concerns at the architecture level may entail describing a combination of computer and network security mechanisms to insure a coherent system for the enforcement of policy. When building a secure system, the designers may take as axioms the trustworthiness of the system security officer, a particular instruction-set architecture and

programming language. Using hardware and software, it is possible to construct a system to insure process isolation and the protection of the operating system. The software developer will be concerned with the effective use of hardware mechanisms to support these objectives. The hardware designer will attempt to construct devices that substantively support protection objectives while admitting a wide variety of software implementations. A hardware designer may assume a particular cell library, memory organization, instruction-set, etc. Security concerns may focus on correctness.

System elements such as processors, operating systems, compilers, databases, networks, etc., are significant application areas for both engineering and security.

Educational Outcomes

- Ability to design and analyze solutions to meet requirements and specifications at multiples levels of abstraction and with several viewpoints.
- Ability to understand the impact actions in one level or viewpoint have on other levels or viewpoints.
- Ability to trade-off several requirements from different view points in order to achieve the maximum benefit.

3.2.4 Empirical Dimensions of Reasoning

The empirical dimension is concerned with experiments and with the results attained on "real" systems. In engineering, empirical results are obtained on the "lab bench" by building prototypes, instrumenting systems, measuring their performance, and by testing and simulation.

All of the above empirical methods are applicable to security. Functional interface testing, internal engineering tests of selected subsystems, system generation and recovery tests, as well as unit and module testing are all part of the development process for a secure system [26]. Hardware may be examined for flaws [41], covert channels analyzed [24, 49], and systematic penetration analyses based on the Flaw Hypothesis Methodology [47] conducted. Analyses are conducted and prototype systems are built and examined for security flaws, such as vulnerability to "real" attacks. Performance issues may also be examined by balancing expected decreases in vulnerability versus user convenience and system efficiency. Techniques for assessing the vulnerability of systems may be used to examine real systems for real flaws.

Educational Outcomes

- Ability to construct experiments or prototypes to demonstrate some purpose or facilitate some meaningful exploration.
- Ability to observe, collect, analyze, and interpret data from experiments.

3.2.5 Conceptual Dimensions of Reasoning

The conceptual dimensions of reasoning define the discipline. In computer engineering and science, the fundamental theoretical concepts are based on mathematics, logic, and physics. The theoretical concepts form the principles of construction and analysis.

In electrical and computer engineering, linear systems theory is based on the sinusoidal composition of signals and on superposition. This gives rise to the classical treatments of networks, controls, and communications theory.

The construction of computer hardware and to a lesser extent software, is based on propositional logic, predicate calculus, discrete mathematics, and finite-state machine theory. Functional programming and object-oriented design depend on type theory.

In addition to applying standard mathematical foundations for constructing hardware and software, security also includes theoretical concepts to support the development and use of cryptography and cryptographic functions; cryptographic protocols; formal policy models; formal specification; and the use of formal methods for verification and covert channel analysis. The means for analysis is based on discrete mathematics, information theory and mathematical logic – such as standard predicate calculus, modal logic, and specialized belief logics.

Educational Outcomes
For each level of design abstraction, application, and for each requirement:

- Clear understanding of the mathematical, logical, and physical concepts which form the analytical basis and principles of construction.
- Ability to apply analytical concepts and principles of construction to the analysis and construction of real systems.

3.2.6 Assumptions Made

The assumptions which are made by each discipline are based on the components, services, and properties assumed to be available for each level of design and frame of reference. Design levels and levels of abstraction are defined by these assumptions as well as the particular rules of composition used for for creating structures of components. For example, designers of authentication protocols assume the presence of encryption functions of suitable strength. Designers of software assume the correctness of the hardware platform supporting the instruction-set architecture. Secure system designers may assume that the System Security Officer/Administrator is trustworthy and that the compiler, placed under configuration management, does not contain artifices to create trapdoors.

A means to check consistency between security and engineering concerns is to check the underlying assumptions made by each set of concerns. Inconsistent assumptions are caused by mismatches in design levels, frames of reference, or applications.

Educational Outcomes
For each level of design abstraction, application, and for each requirement:

- Ability to clearly state assumptions being made.
- Ability to justify the assumptions being made.
- Ability to check the consistency of assumptions being made.

3.2.7 Implications and Consequences

In both engineering and security, the implications and consequences of design decisions and system behaviors have their impact on:

- Risk analysis;
- cost;
- Ease of manufacture;
- Ease of maintenance;
- Reliability; and
- Ethical considerations.

The determination of implications and consequences relies on all the previous elements of the framework. The correct balancing of consequences is sometimes termed as "business sense." Experienced and successful system architects and designers find this correct balance based on experience, empirical reasoning, and conceptual reasoning coupled with a deep understanding of the intended purpose or goal.

Determining the ethical consequences of computer use is complex [5] but may be based on the following criteria in Table **1:**

- An understanding of professional and ethical responsibility;
- The broad education necessary to understand the impact of engineering solutions in a global and societal context; and
- A knowledge of contemporary issues.

Educational Outcomes
- Ability to anticipate and clearly state with precision and accuracy the positive and negative consequences.
- Ability to judge the likelihood of consequences.

3.2.8 Inferences

The elements of Sections **3.2.1** through **3.2.7** are used to infer conclusions about security and systems. Inferences which are made include the determination of:

- Fail secure and secure system recovery;
- Systematic penetration testing and the Flaw Hypothesis Methodology [47]; and
- Detection of and proving abusive behavior based on profiling and audit data.

The above are concerns which are common to both security and engineering.

Educational Outcomes

- Ability to draw correct inferences based on principles, observations, concepts, and data.
- Ability to justify conclusions.
- Ability to draw conclusions which are relevant and consistent.

3.3 Are the Framework and Outcomes Satisfactory?

One way to evaluate the adequacy of the framework and outcomes described in Sections 3.2.1 through 3.2.8 is to compare it to stated requirements for information security education made by computer security experts and accreditation criteria for electrical and computer engineering. We examine the proposed educational framework against the remarks made by employers in the computer security field at the 1996 IEEE Symposium on Security and Privacy [39, 6], the 1997 ACM Workshop on Education in Computer Security [44], and the 1997 National Colloquium for Information Systems Security Education [23], and against the accreditation requirements for electrical and computer engineering proposed by the IEEE.

1. Bill Murray, Senior Vice President, Deloitte and Touch said [23]:

   > "Computer science education with respect to security needs rigor, discipline and sound engineering values."

2. Roger Schell, Senior Development Manager for Information Security, Netware Systems Group, Novell, Inc. [39] asked for individuals who:

   - Understand fundamental computer science concepts; and
   - Can think critically.

3. Jim Schindler, Information Security Program Manager at Hewlett Packard has described security professionals as individuals who are able to adapt and build secure systems in a world of changing technology, changing computer paradigms and changing security requirements [39].

4. John Kauza, Vice President for Security, ATT, provided his list of skills and core competencies as follows, [23]:

   - Ethics;
   - Security orientation;
   - Technical computer science knowledge; and
   - Operational/practical expertise to think and apply to industry.

5. Steve Barnett, of the National Security Agency, [6] made the following points:

   - Security solutions must be sought in the context of changing technology.
   - Focus on the supportive skills in other classes including:

- architecture and design; and
- hardware, software, and protocols for systems and networks.

- Complement formal approaches to security with practical examples and applications.
- Security requires a comprehensive systems approach and students must
  - Be able to state security requirements;
  - Be able to design to meet those requirements;
  - Be able to implement the design correctly;
  - Be able to test designs and implementations; and
  - Be able to manage system configuration and maintenance.

6. Daniel Faigin, of the Aerospace Corporation's Trusted Computer Systems Department, which is involved in testing, security research, and system evaluations, described:

- Basic Skills
  - Fundamental understanding of software engineering techniques;
  - Understanding a specific area such as: operating system design and architecture, information systems security, networks, or database applications; and
  - Good communication skills;
- Supplemental skills
  - Familiarity with secure system evaluation criteria; and
  - Experience with
    * Hardware,
    * Formal mathematical logic,
    * Testing and testing methodologies, and
    * Various languages and operating systems.

Given the above list, we respond to the main points of each as follows.

1. Examining these points, items 1, 2, 3, 4, 5, and 6, all specify that security is not an isolated discipline but part of the larger context of engineering and computer science. The framework relates engineering and security within each element of the framework which covers top-level goals, design, implementation, analysis, and testing.

2. Kauza specifies that ethics be part of security education. This is also part of engineering education and is part of the common framework under *implications and consequences.* However, it is noteworthy that a conclusion emerging from the 1997 WECS [18] was that *information responsibility* should be taught well before students enter institutions of higher education and that the appropriate venue for social, legal and ethical issues associated with computing may be program dependent.

3. Kauza, Faigin, and Schindler require operational expertise applicable to industry. This is covered within the framework under *empirical dimensions* of *reasoning.*

4. The remaining points deal with specific concerns over linking security to several engineering activities spanning requirements, specification, design, implementation, testing, and validation. The proposed framework covers requirements through testing and validation. Barnett's plea for theory to inform practice and practice to inform theory is reflected in both the conceptual and empirical dimensions of reasoning.

Table **3:** Accreditation Criteria for Electrical and Computer Engineering

Proposed Program Criteria for Electrical, Computer, and Similarly Named Engineering Programs

Submitted by the Institute of Electrical and Electronics Engineers, Incorporated

January 16, 1997 (Revised 2/5/97, 2/21/97, 3/4/97, 3/8/97)

These program criteria apply to engineering programs which include electrical, electronic, computer, or similar modifiers in their titles.

Curriculum

Programs must demonstrate that their graduates have achieved the outcomes listed in Criterion **3** in three or more areas of electrical and/or computer engineering as appropriate to the program name and objectives. Graduates must demonstrate knowledge of probability and statistics, including applications appropriate to the program name and objectives. Graduates must demonstrate knowledge of mathematics through differential and integral calculus, basic science, and engineering science necessary to analyze and design complex devices and systems containing hardware and software components and appropriate to program objectives. Graduates of programs containing the modifier electrical in the title must also demonstrate the knowledge of advanced mathematics, typically including differential equations, linear algebra, and complex variables. Graduates of programs containing the modifier computer in the title must also demonstrate knowledge of discrete mathematics.

5. Schell synthesized the requirements by asking for engineers and scientists who are capable of *thinking critically* about security within systems, as opposed to technicians who are merely knowledgeable of security techniques. Placing security and engineering within a framework of critical thinking directly addresses this higher order requirement.

How well does the proposed framework meet the accreditation requirements for engineering? The accreditation criteria for electrical and computer engineering programs proposed by the IEEE is shown in Table **3.** They refer to *Criterion 3* contained in Table **1.** Programs must demonstrate that graduates have:

- Achieved the outcomes listed in Criterion **3** in three or more areas of electrical and/or computer engineering;
- Knowledge and application of mathematics and engineering science necessary to analyze and design complex devices and systems containing hardware and software; and
- Knowledge of discrete mathematics.

All of the above items are contained within the proposed framework. If proper attention is placed to the element of *points of view and frames of reference,* multiple design levels and applications will be addressed.

4 Assessing the Results

Assessment of systems is an accepted practice by the security community. For example, the Trusted Computer System Evaluation Criteria (TCSEC) [25] describe seven system rating classes and their respective functional and assurance requirements. (See Table 4 from Gasser [16]). For consumers, the ratings provide an independent technical assessment of the likelihood that a system contains a flaw that would result in a catastrophic failure to enforce security policy. The objective is to assess systems based on their behaviors, capabilities, and degree of confidence in the implementation.

Class	Title	Key Features
A1	Verified Design	Formal top-level specification and verification, formal covert channel analysis, informal code correspondence demonstration.
B3	Security Domains	Reference monitor (security kernel), "highly resistant to penetration."
B2	Structured Protection	Formal model, covert channels constrained, security-oriented architecture, "relatively resistant to penetration."
B1	Labeled Security Protection	Mandatory access controls, security labeling, removal of security-related flaws.
C2	Controlled Access Protection	Individual accountability, extensive auditing, add-on packages.
C1	Discretionary Security Protection	Discretionary access controls, protection against accidents among cooperating users.
D	Minimal Protection	Unrated.

The problem faced by educators is how to assess the capabilities of students. How do we judge whether students have learned and if so, how much? This is not merely the administration of tests, most of which traditionally assessed lower-order skills such as recall. Rather, the challenge is to see if students are able to "think like an engineer or think like a computer security specialist."

One measure of a successful curriculum is when there is compelling evidence that students who complete a curriculum have achieved the specified educational outcomes. The type of evidence gathered depends on answers to questions such as:

- What are the desired educational outcomes?
- What are some behaviors or indicators which characterize the outcomes?
- What are the underlying principles which are important?
- What are the standards used to judge quality?

Educational assessment is important because it addresses quality. Are students *in fact* learning? Do graduates *in fact* possess the required skills? Assessment is based on the culture of *evidence,*

much as the TCSEC uses coherent groupings of functional properties and assurance evidence to make its assessments. A justification for assessment is found in *Learning through Assessment: A Resource Guide for Higher Education,* [2]:

> Through assessment, educators meet responsibilities to students and to the public. There is a compelling public stake in education. As educators, we have a responsibility to the publics that support or depend on us to provide information about the ways in which our students meet goals and expectations. But that responsibility goes beyond the reporting of such information; our deeper obligation – to ourselves, our students and society – is to improve. Those to whom educators are accountable have corresponding obligation to support such attempts at improvement.

The four principles of assessment put forth by the American Association for Higher Education (AAHE) **[2]** which apply to this paper are:

1. The assessment of student learning begins with educational values.
2. Assessment is most effective when it reflects an understanding of learning as multidimensional, integrated, and revealed in performance over time.
3. Assessment works best when the programs it seeks to improve have clear, explicitly stated purposes.
4. Assessment requires attention to outcomes but also and equally to the experiences that lead to those outcomes.

The framework and outcomes are consistent with and supportive of the above principles. First, the values cited by Reich [31] as supported by the skills of **1)** abstraction, **2)** system thinking, **3)** experimentation and testing, and **4)** collaboration and communication, are elements of the framework and are listed as specific educational outcomes in several elements.

Second, the framework and outcomes are spread over several viewpoints and activities which span all design levels and link theory to practice. The outcomes are likely to be achieved by several sequences of courses through a curriculum over several years and not by a single course in one semester. The framework provides a means to link the various elements across engineering and security.

Third, the framework and outcomes have the explicit purpose of linking engineering and security. The elements of the framework identify common ground between engineering and security which mutually support the outcomes.

Fourth, the framework identifies a variety of experiences and activities as means for meeting the outcomes. Theory and practice are contained as are low-level and high-level design and analysis.

While it is beyond the scope of this paper to develop the precise assessment instruments to be used, the use of critical thinking as a higher-order organizing framework allows for the specialization of assessment tools for critical thinking to the critical framework for engineering and security. Paul and Nosich in [32] provide high-level examples for each of the eight elements of the framework. Tables 6 and **7** are excerpted from [32] as examples. The remaining six are found in [32].

More detail on curricula development and assessment can be found in Diamond's *Designing and Improving Courses and Curricula in Higher Education,* [11].

Table 5: A Partial Listing of Assessment Principles from AAHE

Principles **of** Good Practice **for** Assessing Student Learning

Developed under the auspices of the AAHE Assessment Forum, December 1992

1. The assessment of student learning begins with educational values. Assessment is not an end in itself but a vehicle for educational improvement. Its effective practice, then, begins with and enacts a vision of the kinds of learning we most value for students and strive to help them achieve. Educational values should drive not only what we choose to assess but also how we do ***so.*** Where questions about educational mission and values are skipped over, assessment threatens to be an exercise in measuring what's easy, rather than a process **of** improving what we really care about.
2. Assessment is most effective when it reflects an understanding **of** learning **as** multidimensional, integrated, and revealed in performance over time. Learning is a complex process. It entails not only what students know but what they can do with what they know; it involves not only knowledge and abilities but values, attitudes, and habits of mind that affect both academic success and performance beyond the classroom. Assessment should reflect these understandings by employing a diverse array of methods, including those that call for actual performance, using them over time ***so*** **as** to reveal change, growth, and increasing degrees of integration. Such an approach aims for a more complete and accurate picture of learning, and therefore firmer bases for improving our students' educational experience.
3. Assessment works best when the programs it seeks to improve have clear, explicitly stated purposes. Assessment is a goal-oriented process. It entails comparing educational performance with educational purposes and expectations – those derived from the institution's mission, from faculty intentions in program and course design, and from knowledge of students' own goals. Where program purposes lack specificity or agreement, assessment **as** a process pushes a campus towards clarity about where to aim and what standards to apply; assessment also prompts attention to where and how program goals will be taught and learned. Clear, shared, implementable goals are the cornerstone for assessment that is focused and useful.
4. Assessment requires attention to outcomes but also and equally to the experiences that lead to those outcomes. Information about outcomes is of high importance; where students "end up" matters greatly. But to improve outcomes, we need to know about student experience along the way – about the curricula, teaching, and kind of student effort that lead to particular outcomes. Assessment can help **us** understand which students learn best under what conditions; with such knowledge comes the capacity to improve the whole of their learning.

Table 6: Assessing the Question at Issue or Central Problem, from Paul

Question at Issue or Central Problem
(All reasoning *is* an attempt to *figure* something out, to settle some question, solve some problem)

Fundamental Standards: 1) Clarity of Question, **2)** Significance of Question, **3)** Answerability, **4)** Relevance

Flawed Questions: **1)** Unclear, **2)** Insignificant, **3)** Not Answerable, **4)** Irrelevant

Principle: To settle a question you must understand what it requires

Good Reasoners:	Bad Reasoners:	Feedback to Students:
are clear about the question they are trying to settle	are often unclear about the kind of question they are asking	(-) The main question at issue is never made clear. (+) You did a good job of clarifying the question at issue.
can re-express a question in a variety of ways	express questions vaguely and find them difficult to reformulate	(-) You need to reformulate your question in a couple of ways to recognize the complexity of it. (+) I like the way you reformulate your question in different ways. It helps the reader see it from different points of view.
can break a question into sub-questions	are unable to break down the questions they are asking	(+) You do a good job of analyzing the main question into sub-questions. (-) It would be easier to solve your main problem if you would break it down somewhat.
have sensitivity to the kind of question they are asking routinely distinguish questions of different type	have little sensitivity to the kind of questions they are asking, confuse questions of different types, often respond inappropriately to the questions they **ask**	(-) You are confusing a legal question with a moral one. (+) You do a good job of keeping the economic issues separate from the ***so***cial ones.
distinguish questions they can answer from questions they can't	try to answer questions they are not in a position to answer	(+) You were correct in leaving that question unanswered, and in recognizing what extra information you would need to answer the question

Table *7:* Assessing Inference and Conclusion, from Paul

Inference & Conclusion

***(All* reasoning contains inferences by which we draw conclusions and give meaning *to* data)**

Fundamental Standards: 1) Clarity of Inferences, **2)** Justifiability of Inferences, **3)** Profundity of Conclusions, **4)** Reasonability of Conclusions, 5) Consistency of Conclusions

Failure of **Inferences and Conclusions: 1)** Unclear, **2)** Unjustified, **3)** Superficial, **4)** Unreasonable, 5) Contradictory

Principle: Reasoning can only be **as** sound **as** the inferences it makes and conclusions it comes to

Good Reasoners:	**Bad Reasoners:**	**Feedback to Students:**
make inferences that are clear and precise	often make inferences that are unclear	(-) It is not clear what your main conclusion is. (-) It is not clear what you base your main conclusion on. (+) Your reasoning is very clear and easy to follow.
usually make inferences that follow from the evidence or reasons presented	often make inferences that do not follow from the evidence or reasons presented	(-) The conclusion you come to does not follow from the reasons presented. (+) You justify your conclusion well with supporting evidence and good reasons.
often make inferences that are deep rather than superficial	often make inferences that are superficial	(+) Your central conclusion is well-thought-out and goes right to the heart of the issue. (-) Your conclusion is justified, but it seems superficial given the problem.
often make inferences or come to conclusions that are reasonable	often make inferences or come to conclusions that are unreasonable	(-) It is unreasonable to infer a person's personality from one action.
make inferences or come to conclusions that are consistent with each other	often make inferences **or** come to conclusions that are contradictory.	(-) The conclusions you come to in the first part of your paper seem to contradict the conclusions that vou come to at the end.

5 Discussion of Security Education Programs

Cryptography and the use of cryptographic protocols is appealing as a single-course topic. Many books and texts are available for teaching cryptography and network security, e.g. [45, 37, 43, 15, 22]. Cryptography and its use in secure communication protocols is an important aspect of network security and secure distributed architectures. It is straightforward for an individual to study a small collection of books and papers and become a competent instructor in this area without an extensive apprenticeship in the field. (We note that caution should be exercised when attempting to become a practitioner. The design of good protocols and cryptosystems requires significant expertise [1, 36, 38].)

Despite its appeal, cryptography and its application is only one part of an overall approach to computer and network security; a program confined to cryptography and cryptographic protocols, will be insufficient to convey to students the foundational concepts and design principles that must be followed to successfully build secure systems. Designing and building secure systems involves an understanding of foundational aspects of operating systems, software engineering, modeling, and many other fundamental areas of computer science and engineering, see [10, 30, 46, 35, 3]. The framework described in this paper provides a blueprint for achieving an information security education with an appropriately broad scope.

6 Conclusions

The increasing use, reliance upon, and vulnerability of current large-scale information systems demands that more resilient, reliable, and secure systems be built and deployed. These issues must receive more attention in the education of engineers and computer scientists. Security concepts are fundamental ones which apply to all levels of system design and application. As such, technically meaningful ways must be sought to integrate security into the engineering and computer science curricula charged with the education of the majority of system designers and implementors. Some undergraduate programs will offer specialized courses in computer security and graduate programs can provide advanced security courses complemented by research. These focussed courses and programs will be attractive to only a subset of the student population; they do not reach the vast majority of students. A compounding factor will be the inability of many programs to add one or more security courses to already overcrowded curricula. It is unreasonable to create separate security curricula isolated from those of engineering and computer science. A reasonable approach is to integrate security concerns in technically meaningful ways into engineering and computer science curricula.

Using the critical framework of Section 3, the technical aspects of security are found to be closely related to computer engineering and science. As many of the goals, concepts, and means of reasoning are similar, it seems both desirable and practical to incorporate elements of each into the disciplines of security and computer engineering and science.

Ideally, course material in the form of text books and laboratory examples would have computer engineering and science integrated with security. The Air Force Academy provides an example of a curriculum into which security has been integrated by explicitly injecting security topics into introductory courses on operating systems, databases, software engineering, and networks [48]. This approach has the advantage of viewing security as an important application and property which is an integral part of computer engineering and science. At institutions where this is not immediately

possible, security-related supplements can be added to each category in computer engineering and science. The framework and outcomes-based assessment can be used to ensure coherence and coverage of security skills within an engineering curriculum. As engineering programs are now accredited using outcomes-based assessment, institutions which wish to distinguish themselves by virtue of having an information security focus can do so and be recognized and accredited for their efforts.

References

[1] Martin Abadi and Roger Needham. Prudent Engineering Practice for Cryptographic Protocols. In *IEEE Symposium on Research in Security and Privacy*, pages 122 – 136, Oakland, CA, May 1994.

[2] American Association for Higher Education Assessment Forum. *Learning Through Assessmement: A Resource Guide for Higher Education*, 1997.

[3] Edward Amoroso. *Fundamentals of Computer Security Technology*. Prentice Hall Publishing, Englewood Cliffs, NJ, 1994.

[4] James P. Anderson. Computer Security Technology Planning Study. Technical Report ESD-TR-73-51, Air Force Electronic Systems Division, Hanscom AFB, Bedford, MA, 1972. (Also available as Vol. I,DITCAD-758206. Vol. II, DITCAD-7728 06).

[5] Sarah Baase. *A Gift of Fire: Social, Legal, and Ethical Issues in Computing*. Prentice Hall, Englewood-Cliffs, NJ, 1997.

[6] Steve Barnett. Computer Security Training and Education: A Needs Analysis. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 26 – 27, Los Alamitos, CA, May 1996. IEEE Computer Society Press.

[7] Defense Science Board. Report of the Defense Science Board Task Force OR Information Warfare – Defense (IW-D). Technical report, Office of the Secretary of Defense, November 1996.

[8] D. L. Brinkley and R. R. Schell. Concepts and Terminology for Computer Security. In Abrams, Jajodia, and Podell, editors, *Information Security: An Integrated Collection of Essays*, pages 40 – 97. IEEE Computer Society Press, Los Alamitos, CA, 1995.

[9] Computer Science Accreditation Commission (CSAC). Criteria for Accrediting Programs in Computer Science in the United States.
URL http://www.cse.fau.edu/~roy/csab97/criteria96_2.html#P2.

[10] Dorothy E. Denning. *Cryptography and Data Security*. Addison Wesley Publishing, Reading, **MA,** 1982.

[11] Robert M. Diamond. *Designing and Improving Courses and Curricula in Higher Education*. Jossey-Bass, San Francisco, 1989.

[12] Engineering Accreditation Commission of The Accreditation Board for Engineering and Technology. *Engineering Criteria* 2000, for review and comment – second edition.

[13] Engineering Deans Council, Corporate Roundtable, American Society for Engineering Education. *Engineering Education* for *a Changing World,* October 1994.

[14] National Coordination Office for HPCC. Committee on Information and Communications (CIC) Strategic Implementation Plan.
URL http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/cic/cic_plan.html.

[15] Warwick Ford. *Computer Communications Security.* Prentice Hall Publishing, Englewood Cliffs, NJ, 1994.

[16] Morrie Gasser. *Building a Secure Computer System.* Van Nostrand Reinhold, New York, 1988.

[17] Diane F. Halpern. *Thought and Knowledge: An Introduction to Critical Thinking.* Lawrence Earlbaum Associates, New Jersey, third edition, 1996.

[18] Heather Hinton. Review of First Annual Workshop on Education in Computer Security. *Electronic CIPHER, Issue 21,* March 1997.
URL http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/issue9703 .

[19] Cynthia E. Irvine. Goals for Computer Security Education. In *Proceedings* of *the IEEE Symposium on Security and Privacy,* pages 24 – 25, Los Alamitos, CA, May 1996. IEEE Computer Society Press.

[20] Cynthia E. Irvine. Challenges in Computer Security Education. *IEEE Software,* pages 110 – 111, September/October 1997.

[21] Cynthia E. Irvine, Daniel F. Warren, and Paul C. Clark. The NPS CISR Graduate Program in INFOSEC: Six Years of Experience. In *Proceedings* of *the 20th National Information Systems Security Conference,* pages 22 – 30, Baltimore, MD, October 1997.

[22] Charlie Kaufman, Radia Perlman, and Mike Speciner. *Network Security, Private Communication in a Public World.* Prentice Hall Publishing, Englewood Cliffs, NJ, 1995.

[23] John Kauza. Industrial Perspective on INFOSEC Education Requirements. In *Proceedings* of *the National Colloquium for Information Systems Security Education,* pages 76 – 80, Maritime Institute of Technology, Linthicum, MD, April 23 – 24 1997.

[24] Richard Kemmerer. Shared Resource Matrics Methodolgy: A Practical Approach to Identifying Covert Channels. *ACM Transactions on Computer Systems,* 3(1):256–277, August 1983.

[25] National Computer Security Center. *Department* of *Defense Trusted Computer System Evaluation Criteria,* December 1985. DoD 5200.28-STD.

[26] National Computer Security Center. *Final Evaluation Report* of *Gemini Computers, Incorporated Gemini Trusted Network Processor, Version 1.01,* 28 June 1995.

[27] President of the United States. Executive order 13010, 1997.
URL http://www.pccip.gov/eo13010.html.

[28] Presidental Commission on Critical Infrastructure Protection. Report summary, critical foundations, thinking. differently.
URL **http://www.pccip.gov/summary.html.**

[29] Charles Pfleeger and Deborah Cooper. Security and Privacy: Promising Advances. *IEEE Software,* pages 27 – 32, September/October 1997.

[30] Charles P. Pfleeger. *Security in Computing, Second Edition.* Prentice Hall, Inc., Englewood Cliffs, NJ, 1996.

[31] Robert Reich. *The Work of Nations.* Vintage, New York, NY, 1992.

[32] Richard Paul and Gerald M. Nosich. Using Intellectual Standards to Assess Student Reasoning. In Jane Willsen and A.J.A. Binker, editors, *Critical Thinking: how to prepare students for a rapidly changing world,* pages 153 – 164. Foundation for Critical Thinking, 1995.

[33] Richard Paul and Jane Willsen. Accelerating Change, the Complexity of Problems, and the Quality of Our Thinking. In Jane Willsen and A.J.A. Binker, editors, *Critical Thinking: **how** to prepare students for a rapidly changing world,* pages 1 – 16. Foundation for Critical Thinking, 1995.

[34] Richard Paul and Jane Willsen. Critical Thinking: Identifying the Targets. In Jane Willsen and A.J.A. Binker, editors, *Critical Thinking: how to prepare students for a rapidly changing world,* pages 17 – 36. Foundation for Critical Thinking, 1995.

[35] Deborah Russell and G.T. Gangemi. *Computer Security Basics.* O'Reilly and Associates, Inc., Sebastopol, CA, 1991.

[36] Bruce Schneier. Why Cryptography Is Harder Than It Looks.
URL **http://www.counterpane.com/whycrypto.html.**

[37] Bruce Schneier. *Applied Cryptograhpy.* John Wiley and Sons, New York, NY, 1996.

[38] Bruce Schneier. Cryptography, Security, and the Future. *Comm. A.C.M,* 40(1), January 1997.

[39] Christoph L. Schuba and Mary Ellen Zurko. IEEE CS Symposium on Security and Privacy, Electronic CIPHER, Issue 15, 1 June 1996.
URL **http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/issue9606**

[40] Computer Science and National Research Council Telecommunications Board. *Cryptography's Role in Securing the Information Society.* National Academy Press, 1996.

[41] Olin Sibert, Phillip A. Porras, and Robert Lindell. The Intel 80x86 Processor Architecture: Pitfalls for Secure Systems. In *Proceedings **1995** IEEE Symposium on Security and Privacy,* pages 211–222, Oakland, CA, May 1995. IEEE Computer Society Press.

[42] Eugene H. Spafford. Testimoney before the United States House of Representatives' Subcommittee on Technology, Computer and Network Security.
URL **http://www.house.gov/science/hearing.htm.**

[43] William Stallings. *Network and Internetwork Security Principals and Practice.* Prentice Hall Publishing, Englewood Cliffs, NJ, **1995.**

[44] Christine Stevens and Daniel Faigin. Position Statement and Presentation for the First ACM Workshop on Education in Computer Security. Monterey, CA, January **1997.**

[45] Douglas R. Stinson. *Cryptography Theory and Practice.* CRC Press, New York, NY, **1995.**

[46] Rita Summers. *Secure Computing.* McGraw Hill, New York, NY, **1997.**

[47] Clark Weissman. Penetration Testing. Technical report, Naval Research Laboratory, January **1995.** NRL Technical Memorandum **5540:082A.**

[48] Gregory White and Gregory Nordstrom. Security Across the Curriculum: Using Computer Security to Teach Computer Science Principles. In *Proceeding of the 19th National Information Systems Security Conference,* pages **483** – 488, Baltimore, MD, October **1996.**

[49] J.C. Wray. **An** analysis of covert timing channels. In *Proceedings 1991 IEEE Symposium on Research in Security and Privacy,* pages **2–7.** IEEE Computer Society Press, **1991.**

Initial Distribution List

		No. of Copies
1.	Defense Technical Information Center 8725 John J. Kingman Rd., STE 0944 Ft. Belvoir, VA 22060-6218	2
2.	Dudley Knox Library, Code 52 Naval Postgraduate School Monterey, CA 93943-5100	2
3.	Research Office, Code 09 Naval Postgraduate School Monterey, CA 93943-5000	1
4.	Dr. Blaine Burnham ATTN: R23 National Security Agency 9800 Savage Road Fort George G. Meade, MD 20755-6000	10
5.	Professor Shiu-Kai Chin 2-133 Center for Science and Technology Electrical Engineering & Computer Science Syracuse University Syracuse, NY 13244-4100	3
6.	Professor Cynthia E. Irvine Code CS/Ic Department of Computer Science Naval Postgraduate School Monterey, CA 93943-5118	3
7.	Professor Deborah Frincke Department of Computer Science University of Idaho Moscow, ID 83844-1010	3