

*Integration of Software Security Model  
in Existing Introductory Technology  
Courses*

**Linda A. Walters**

**Technical Report #NSUCS-2004-004  
Norfolk State University  
Department of Computer Science**

**Table of Contents**

Abstract .....1

I. Introduction.....2

II. Background..... 2-3

III. Security and the U.S. Government.....4-5

IV. Computer Security Concepts.....5-7

V. Computers and Business.....7

VI. Future Work.....7-8

## **ABSTRACT**

Secure software is software whose integrity, confidentiality, and availability are maintained. During the current technology era enormous security flaws have been introduced in software primarily due to the lack of understanding on software security. Once secure software has been developed, users are rarely educated on its' use or the importance of its' security features. It is extremely difficult to characterize any software as being totally secure, as any level of security is dictated by the sensitivity of data and often security controls minimize a system's performance. The fundamental question that lies before us is how non-technical individuals can be exposed to software security in a manner that will allow them to understand basic security concepts in order to equip them with the necessary tools to properly utilize secure software. This paper will address the importance of integrating a basic security model as part of a required technology course.

## **I. INTRODUCTION**

The year 2001 redefined our nation's position on national security. Although the terrorist attack on the World Trade Center was of utmost scrutiny, the Internet community was also confronted with a number of cyber attacks that exceeded all previous years combined. As a result, a huge emphasis was placed on Homeland Security thereby changing the population's perspective on the importance of safety measures. These exploits resulted in astronomical financial losses for corporate, government, and private entities. The scope of destruction had no boundaries, as these malicious intrusions spread on a global level in a matter of hours causing enormous damage, loss of data, and downtime. Since the Internet is a global means of communication, not only must one be suspect of malicious attacks but also of identity theft and the exchange of private information. There are many lessons to be learned, and one of utmost importance is the need to educate all non-technical students on the importance of computer security by exploring techniques on how to safeguard information.

## **II. BACKGROUND**

Computer Science is a young but very rapidly growing field that interrelates with all other disciplines in some way. Within the last fifty years the evolution of technology has distinctly identified computer skills as essential in all aspects of business. Currently, most post-secondary institutions require students to participate in at least one technology course in order to equip them with computing concepts that can be applied to their own

disciplines [10]. Since its inception as a distinct discipline, computer science has evolved tremendously due to the increased use of computer systems.

In the 1970s the use of computers was limited to businesses since they were very expensive. During this period only a very basic knowledge of computer technology was required in order to introduce individuals to computer careers. During the early 1980s' computers became affordable introducing personal computers. By the mid 1980's software designers introduced new computer applications such as spreadsheets, work processors, and graphics. Organizations began associating the skills needed to use these software packages with productivity and as employment requirements. Unbeknown to many, the concept of networking had been introduced in 1962 and became very important to researchers ultimately developing into the Internet as we know it today. The Internet, a network of networks based on standards and infrastructure, has revolutionized the way people communicate, shop, bank, and search for information throughout the world. Although much has occurred in relation to technology within the last fifty years it is safe to say that the development of different technologies has dictated the amount of literacy required to function in a computerized world [1]. It is therefore impossible to increase computer security awareness without incorporating technical skill [9].

Today computers are not considered a luxury but a necessity. Most individuals conduct business transactions, research, and chat via the World Wide Web. As such, individuals must be educated in the dangers of exchanging personal information to prevent identity theft and fraud. Computer security is a topic that has been explored since the 1970s' although it had not gained a level of importance as it has in recent years. With the prevalence of computer intrusion, crimes, and Internet usage educators bear the

responsibility of building a new generation of graduates prepared with the appropriate knowledge and skills to unravel security issues.

### **III. SECURITY AND THE U.S. GOVERNMENT**

Protecting information has been a challenge since the beginning of the computer age, as computer technology for business operations has been widely adopted. Also, the widespread use of the Internet has increased security awareness, as interconnectivity is responsible for the spreading of viruses. One example is the 1999 Denial of Service attack on e-commerce sites where the vulnerability existed among the protocols that were utilized to communicate via the Internet. Unfortunately, the ability to communicate with many different systems opens the door to intruders who can cripple the very protocols intended to establish a connection. A brief history of actions the United States Government has taken explains the importance of computer security. Several computer security related documents have had a great impact on the US legislation and governmental structure. These documents include the Computer Security Act of 1987 which assigned the responsibility of developing security and privacy of sensitive information guidelines for Federal computer systems to the National Bureau of Standards; the Joint Security Commission's 1994 report stated that "the security of information systems and networks is the major security challenge of this decade and possibly the next century"; the 1996 Executive Order 13010 where the President ordered the establishment of the President's Commission on critical Infrastructure Protection (PCCIP) consisting of members of 10 executive branch departments and agencies; the Critical Infrastructure Assurance Office, the National Information Protection Center and

the Information Sharing and Analysis Center established in 1998 as part of the Presidential Decision Directive 63 officially expanded the US national policy to include the cyber world; the Secretary of Defense's 1998 Annual Report to the President and the Congress named a new center, the Information Operations Technology Center established to coordinate interagency information operations and information operations were defined as 'actions taken across the entire conflict spectrum to affect adversary information and information systems while protecting one's own information and information systems.' Information assurance was defined as protecting and defending information and information systems by ensuring their availability, integrity, authenticity, and confidentiality. Finally in 1999, the National Security Agency issued a press release designating seven universities as the first Centers of Excellence in Information Assurance under the Centers of Excellence Program.

I submit that a security model should be implemented that focuses on law, ethics, physical security, business continuity and disaster recovery. The drawback of instituting such a model is that there is a lack of computer security education among educators. Therefore, institutional support is required to provide funds for training and research in order to bring educators up to par with computer security [12].

#### **IV. COMPUTER SECURITY CONCEPTS**

Computer security entails keeping anyone from doing things you do not want them to do, with, on, or from computers or any peripheral devices. The security of any computer system is based on an entity's needs, which is the first step in designing a security policy. As there is no such thing as a full proof security system users must be

aware of three fundamental security concepts: confidentiality, integrity, and availability. Confidentiality refers to limiting the number of authorized individuals being able to access protected data. Integrity refers to maintaining the preciseness and accuracy of data. Availability refers to making information accessible only to individuals that have a need to view the information.

Computing systems can experience vulnerabilities in three broad categories: hardware, software, and data. For the purpose of this report I will discuss data vulnerabilities at length in order to expound on the necessity of educating students on the importance of safeguarding information. In regards to data, confidentiality prevents unauthorized disclosure of a data item, integrity prevents unauthorized modification, and availability prevents denial of authorized access. Data is a major security concern and poses a more prevalent threat, as it is visible in nature and can be easily interpreted. Although data within itself is hard to measure individuals that are familiar with certain information can manipulate data to cause a loss of revenue, life, or an organization's competitive edge. In comparison to hardware and software, data items may have great value but for a short time since information can change daily. As a result, data security has a direct correlation with the principle of adequate protection where computer items must be protected only until they lose their value as well as being protected to a degree consistent with their value. Data confidentiality can easily be compromised by tapping wires, bribing key employees, requesting data, and by inferring the sensitivity of data through non-sensitive data. Compromising data integrity can be accomplished by stealing, buying, finding, or hearing sensitive information and in turn utilizing the information for personal gain [14]. There are many things that computer specialists take

for granted that ordinary users are not taught such as the proper way of developing a password or walking away from their terminals while sensitive information is on their computer screens.

## **V. COMPUTERS AND BUSINESS**

All organizations require the use of computers to formalize, systemize, and automate information processes. Businesses employ computer systems to store and compile sensitive information therefore, it is essential to teach students of all disciplines basic computer security concepts in order to protect an organization's assets. Computer education has become an integral part of the entire educational system and as such has been integrated into different curricula to produce professionals that not only possess knowledge in the specialized area but can also utilize computing systems to perform their duties. Also, the link between computers and business is defined by the number of computer applications that have been developed in almost every discipline [6].

Technology has basically revolutionized the way business is conducted throughout the world. The integration of computing systems has increased productivity, improved business performance and have created value for consumers. As such, the need to acquire technical skills along with acquiring familiarity with security concepts will become essential tools to possess.

## **VI. FUTURE WORK**

Computer science will continue to interact with other disciplines, as more technologies will be developed to interact with all disciplines. Pursuant to the *Panel on*

*Integrating Security Concepts into Existing Computer Courses* conducted in March 2002 the general view of the panel participants was that computer security is an essential component in raising awareness of threats, vulnerabilities, and risks, as the subject has reached the point of public awareness [2]. My future work consists of analyzing existing security models and assessing deficiencies in order to develop a module that can be integrated into different curricula. I will also develop a web site that will include a preliminary survey and online simulations through which users will be provided with a series of tasks to measure their computer security knowledge, and ability to use secure software. I plan to test two groups of individuals: technical and non-technical users.

## *Bibliography*

- [1] Hoffman, M. and J. Blake. *Computer Literacy: Today And Tomorrow*. 2003, Quinnipiac University.

History of teaching computer literacy and its relationship with the broad topic of Information Literacy. Includes the description of a course on the Internet that serves as a model for an updated technology literacy course incorporating both computer literacy and information literacy.

- [2] Mullins, P., E. Wynters, J. Wolfe, W. Calhoun, W. Oblitey, M. Fry, and R. Montante. *Panel on Integrating Security Concepts into Existing Computer Courses*. SIGCSE Bulletin (ACM) 1, (August 2002), 365–366.

Panel participants share position statements on security related content in computer courses being improved.

- [3] Tucker, A.B. and P. Wegner. *New Directions in the Introductory Computer Science Curriculum*. Communications of the ACM (August 2003), 11-15.

Review of the evolution of curriculum development, examines alternative curricular approaches, and explores new trends in the design of introductory computer science courses.

- [4] ACM Curriculum Committee on Computer Science, *Curriculum 68 – Recommendations for the Undergraduate Program in Computer Science*, Communications of the ACM 22, 3 (March 1979), 147-166.

Curriculum '68 serves as a fundamental source document for the establishment of computer science education in the United States.

- [5] ACM Curriculum Committee on Computer Science, *Curriculum 78 – Recommendations for the Undergraduate Program in Computer Science*, Communications of the ACM 11, 3 (March 1968), 151-197.

The core curriculum common to all computer science undergraduate programs is presented in terms of elementary level topics and courses, and intermediate level courses.

- [6] *Education Related To The Use Of Computers In Organizations Position Paper – ACM Curriculum Committee on Computer Education for Management*, Communications of the ACM 14, 9 (September 1971), 573-588.

This position paper provides a framework for a study The ACM Curriculum Committee on Computer Education for Management conducted on curriculum development in management information systems education in colleges and universities. The initial approach was to describe the education necessary for the effective use of computers in organizations.

[7] Amarel, S. *Computer Science: A Conceptual Framework for Curriculum Planning*, Communications of the ACM 14, 6 (June 1971), 391-401.

Two views of computer science are considered: a global view which attempts to capture broad characteristics of the field and its relationships to other fields, and a local view which focuses on the inner structure of the field. Also discusses the expectation that computer science will continue to increase its working contacts with other disciplines.

[8] Gabbert, P. *Discipline Focused Non-Major Computer Science Courses*, JCSC 19, 3 (January 2004), 181-188.

Furman University developed and implemented an approach for the non-major course to offer sections that are restricted to specific majors. The paper describes how these sections are organized and evaluates the advantages and disadvantages to this approach.

[9] Wainwright, R.L. *An Introductory Computer Science Course For Non-Majors*. 1980, The University of Tulsa.

Describes an approach to an introductory computer science course designed especially for students who are not specifically required to take a computer course and thus ordinarily receive no appreciation for computers or computing.

[10] Spooner, D.L. and M.M. Skolnich. *Science And Engineering Case Studies in Introductory Computing Courses for Non-Majors*, SIGCSE, ACM Press (April 2002), 154-158.

Paper relates experience in exploiting a science and engineering case study approach to teach introductory computing concepts in a course for non-majors.

[11] Bacon, T. and R. Tikekar. *Experiences With Developing a Computer Security Information Assurance Curriculum*, Journal of Computing in Small Colleges, 16, 2 (April 2003), 254-267.

Paper describes the process of creating a computer security and information assurance curriculum Bachelors degree.

[12] Yang, A.T. *Computer Security And Impact on Computer Science Education*, JCSC, 16, 4 (May 2001), 233-246.

A survey of the computer security field by examining the sequence of actions that the US government has taken since 1987 to counter computer security issues. A comprehensive approach of integrating computer security into an existing degree program.

[13] Tucker, A.B. *Strategic Directions in Computer Science Education*, Communications of the ACM 28, 4 (December 1996), 836-845

The computer science curriculum faces constant evolutionary pressure to integrate new critical developments. The rapid changes in technology also affect the process of educational delivery.

[14] Ware, H. Ware. *Security in Computing*. Upper Saddle River, New Jersey. 2003.