A Multidisciplinary Electronic Commerce Project Studio for Secure Systems

Annie I. Antón*
Department of Computer Science
College of Engineering
North Carolina State University
Engineering Graduate Research Center 408
Raleigh, NC 27695-7534
+1.919.515.5764
+1.919.515.7925 (fax)
aianton@mindspring.com

Julia B. Earp
Department of Business Management
College of Management
North Carolina State University
Campus Box 7229
Raleigh, NC 27695-7229
+1.919.513.1707
Julia_Earp@ncsu.edu

Submitted to the GENERAL track of NCISSE 2000

March 29, 2000

* Corresponding author

A Multidisciplinary Electronic Commerce Project Studio for Secure Systems

Annie I. Antón, *Department of Computer Science, North Carolina State University*
Julia B. Earp, *Department of Business Management, North Carolina State University*

Abstract

While the Internet serves as a virtual marketplace that is dramatically changing the way business is conducted, security and privacy issues are of deeper concern than ever before. The evolutionary nature of electronic commerce systems, highlights the need for conceptual support for requirements discovery, elaboration and validation. Moreover, there is great need for mechanisms to provide practitioners with more formal approaches for determining and assessing the security and privacy needs of electronic commerce systems.

This paper focuses on the authors' efforts to integrate core research and educational objectives. Our research addresses a number of important issues in the design and evolution of electronic commerce systems. The ultimate goal of our work is to demonstrate viable solutions for supporting the early stages of the software lifecycle, specifically addressing the need for novel approaches to ensure security and privacy requirements coverage.

We seek to provide increased visibility into the tasks and process of requirements engineering for evolutionary systems in which policy considerations play a major role. Students, at the undergraduate and graduate level, as well as industrial participants, will employ goals and scenarios throughout the design of electronic commerce systems while applying software engineering principles. A research engine will be used to collect data across various projects with a unique focus on security policy and privacy policy development and their operationalization into system requirements. Practitioners will benefit from stronger guidelines and tools for ensuring requirements coverage as well as from a library of reusable goal classes for software systems in which security and privacy are paramount. The educational objectives include the development of multidisciplinary systems design experiences for students in the form of an undergraduate level project studio specializing in the analysis and design of state of the art electronic commerce systems.

Bios:

Annie I. Antón is the Asea Brown Boveri Assistant Professor of Software Engineering in the College of Engineering at North Carolina State University, where she is a member of the Center for Advanced Computing and Communication. Her research interests include requirements engineering, feature evolution and the design of electronic commerce applications. Antón received her B.S., M.S. and Ph.D. in computer science from the Georgia Institute of Technology. She is a member of the IEEE Computer Society and ACM.

Julia B.Earp is an assistant professor of information technology in the College of Management at North Carolina State University, where she is co-director of the NCSU Internet Security and Privacy Project. She received her Ph.D. in information technology from Virginia Tech and has industry experience involving software development and database programming. She has authored articles on network security, privacy, routing and artificial intelligence. She is a member of the IEEE Computer Society, ACM, AIS and DSI.

A Multidisciplinary Electronic Commerce Project Studio for Secure Systems

Annie I. Antón
Department of Computer Science
College of Engineering
North Carolina State University
Engineering Graduate Research Center 408
Raleigh, NC 27695-7534
+1.919.515.5764
aianton@mindspring.com

Julia B. Earp
Department of Business Management
College of Management
North Carolina State University
Campus Box 7229
Raleigh, NC 27695-7229
+1.919.513.1707
Julia_Earp@ncsu.edu

ABSTRACT

Multidisciplinary systems design experiences are under development for students at North Carolina State University (NCSU) in the form of a project studio specializing in the analysis and design of state of the art electronic commerce systems. The initiative seeks to integrate core research and educational objectives. The research addresses a number of important issues in the design and evolution of electronic commerce systems. The ultimate goal of our work is to demonstrate viable solutions for supporting the early stages of the software lifecycle, specifically addressing the need for novel approaches to ensure security and privacy requirements coverage. Students, at the undergraduate and graduate level will participate in the design of electronic commerce systems while applying software engineering principles in the NCSU electronic commerce project studio.

I. INTRODUCTION

Initially, corporate presence on the Internet provided the public with a wide range of organizational information, (e.g., annual reports, product and service information [AP98]). However, the abundance of new hardware and software technologies has opened the door for organizations to use the Internet to engage in electronic transactions. The Internet is facilitating the growth of electronic commerce; however, there remain many problems and challenges that we seek to address. Technology problems of slow modem access and congestion are common, but are receiving widespread attention via new technologies such as ADSL (Asymmetrical Digital Subscriber Line) and intelligent routing. In contrast, software problems relating to privacy and security pose a much greater challenge for researchers and software practitioners. There is a great need for qualified individuals to develop secure electronic commerce systems and to keep pace with the explosive growth of electronic commerce. To this end, researchers at North Carolina State University (NCSU) are actively engaged in various electronic commerce efforts ranging from applied research to providing graduate students with an innovative and cutting edge curriculum that responds to the workforce needs of the digital economy. However, there is little offered at the undergraduate level to increase the skills and qualifications of our graduates seeking careers in electronic commerce technology, specifically in developing secure electronic commerce systems. The NCSU project studio, discussed in this paper, will guide students using an innovative approach to address security and privacy protection during the early stages of the software development process of electronic commerce systems.

Most organizations involved in electronic commerce collect and transmit sensitive information, applying internal privacy policies and security measures to ensure that this information is protected. Although there are occasional needs to disclose information, effective security measures prevent the damage that could result from unauthorized access to sensitive information, including its unauthorized destruction, modification or disclosure. Whenever sensitive information is exchanged, it should be transmitted over a secure channel and stored securely using technologies such as

encryption, firewalls and access control. Data protection has regrettably subsisted as an afterthought when designing new systems; however, it is rapidly becoming a critical development concern.

Researchers in the security community [Lic97, SM99] highlight the immediate need to address key issues within the research community. Specific challenges for policy research [Lic97] include the need to: 1) address the ill-defined content and structuring of content in policy development, and 2) explore this area with empirical work. Whereas in software, Shimeall et.al. [SM99], highlight the increasing need for software applications to be written with more concern for security to thwart the potential for vulnerabilities often exploited by attackers. In particular, they pose several challenges for research: 1) proper configurations of firewalls, encryption, and authentication for systems and applications, and 2) strengthened efforts towards educating new programmers and designers about security issues. Students will address these challenges in the electronic commerce project studio.

II. STUDIO DESCRIPTION

We are currently establishing an electronic commerce project studio in which undergraduate students, possessing various educational backgrounds, will collaborate and work cooperatively while developing real-world electronic commerce software applications. The underlying research focuses on improving the educational methods and techniques that enable all students to write quality software for new, poorly understood, emerging technologies. Additionally, we seek to increase the scientific basis of software engineering by developing new, more appropriate software process models for the electronic commerce application domain. The state of software engineering education will be advanced due to this new, multidisciplinary approach to entrepreneurial software development in which students will learn to employ more reliable processes to build secure software. The studio is expected to increase information technology literacy and skills among a wide array of students enrolled in non-technical degree programs while exposing computer science and engineering students to issues surrounding management of technology, policy, strategic planning, marketing, group dynamics and leadership. In today's global economy, success is determined not only by technological skills and savvy but by one's ability to work effectively and advantageously given the diversity of skills and background within a project team. The electronic commerce project studio will formalize our approach to multidisciplinary project-based learning while avoiding some of the pitfalls of current software engineering project-based laboratories.

Development and planning activities for the project studio will entail the developing software process and project management educational materials as well as guides (including a full suite of software documentation templates) specifically targeted at rapid development lifecycles for emerging technologies. While this effort focuses on a specific emerging technology, electronic commerce, a broader objective is to ensure tailorability of all guides and materials for future emerging technologies and all transaction-based information systems that require a secure foundation. Additionally, we are establishing a multidisciplinary project course sequence and securing corporate partnerships for the studio, obtaining gifts in kind in the form of hardware and software to support the initiative. Plans include the collection of data on software engineering activities in a series of real electronic commerce projects for actual clients in various domains, sites and project teams. As discussed in Section III, the studio will informally serve as an experimental research engine, allowing us to validate the appropriateness and efficacy of specific software process models, software engineering methods and techniques as well as network security and privacy technologies.

A. Multidisciplinary Education

The ability to draw upon real experiences and one's own relevant research directly affects the quality of teaching. Students need to be able to understand how one's course work has the potential to make a real and immediate impact. This ability to observe the impact of one's work directly affects the quality of learning. To that end, we strive to provide our students with the

ability to grasp the "big picture" and develop those skills that will prepare them for the "real world." At NCSU we seek to accomplish this by teaching principles in the context of working on real problems. The software engineering education literature provides numerous examples of successful project-based learning environments for undergraduate computer science students [DJS96, OM94]. In particular, [Cow98] focuses on the need for a more interdisciplinary approach highlighting similarities and differences between traditional information systems and computer science curricula.

Students in traditional MIS curricula, in which management students take a few computing courses and CS students take a few management courses, do not adequately prepare students to make use of information technology for effective decision making, optimizing management processes, and strategic planning. A management curriculum must reflect the recent advancements in computer technology, networking and database management that are increasingly applicable to solving complex problems in public and private organizations. Similarly, any computer science curriculum must expose students to issues surrounding, for example, management of technology, strategic planning, policy formation, marketing, group dynamics and leadership, bridging the gap between both fields.

Since electronic commerce is of concern and interest to both management and computer science students, it provides a unique application domain in which to actively engage students with multidisciplinary backgrounds [DHH99].

B. Prerequisites for Participation

Although an electronic commerce course for undergraduates (CSC 495E) is currently offered at NCSU, the demand and interest for the course is so overwhelming that students desire additional opportunities to further their studies and experiences in developing secure systems. Thus, there exists great interest in the project studio and its multidisciplinary nature is intentional to attract students from various disciplines at NCSU. Ideally, each team of students, developing electronic commerce systems in the studio, will include representation from the following colleges at NCSU: Management, Engineering and Design. These three colleges, when combined, offer students possessing unique skills for developing the secure applications used for electronic commerce. Incorporating such a variety of backgrounds, skills and students requires an explicit outline for defining qualified students in each college. Figure 1 summarizes the curriculum prerequisities for students entering the studio from each of the three colleges. Qualified students from the College of Management will have completed the prerequisite courses: Management Information Systems (BUS340) and Business Data Communications and Networking (BUS495b). These students will have knowledge regarding networking and security technologies, as well as the underlying managerial and privacy issues present in electronic commerce. College of Engineering students will have completed the following prerequisite courses: Programming Concepts (CSC114), Advanced Programming Concepts (201), Data Structures (CSC311), and Software Engineering (CSC310). These students will have advanced programming and software project management skills. Students enrolled in the College of Design will have completed the prerequisite course, Human-Centered Design (ID445). While students from each of these majors will have different skills and backgrounds, they each bring unique skills which collectively provide a student team with the broad range of skills and background necessary for a successful development team. These students will have the knowledge required to design user-centered interfaces for the electronic commerce applications.

C. Support for Research Investigations

The electronic commerce project studio will employ the use of web-based tool support for scenario management and evolution that is currently under development at NCSU. The tool, named SMaRT (Scenario Management and Requirements Tool), serves as an instrument to collect data on requirements engineering activities and within the context of this studio, the tool will support non-traditional requirements activities such as security policy formation and the identification of enabling technologies to

ensure security and privacy. The availability of SMaRT enables us to conduct focused research that involves:

- Refining and extending the Goal-Based Requirements Analysis Method (GBRAM) [Ant97] by developing heuristics to support security policy formation in the design of transaction-based information systems (Section III).
- Conducting empirical studies of multidisciplinary undergraduate teams employing software, security, and networking technologies to design and develop electronic commerce applications. These studies will be conducted in a project-based learning environment in collaboration with representatives from industry.

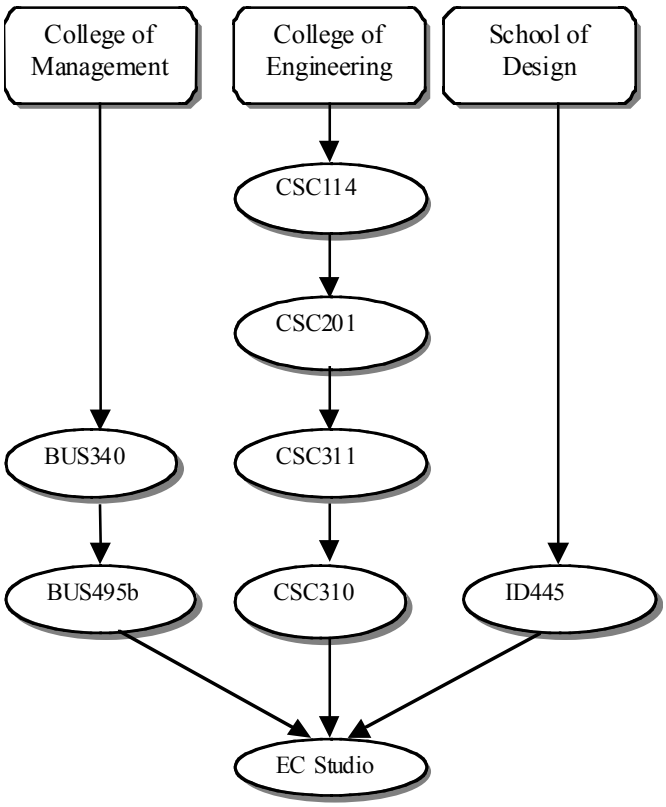

Figure 1: Curriculum Requirements for NCSU Electronic Commerce Project Studio

D. Studio Developmental Timeline

The development plan for the project studio follows:

2000-2001: Prepare materials (Web-based lectures on networking, security, policy, privacy, software engineering, etc.) for the studio. Obtain hardware and software to equip the studio. Develop and validate new policy identification and formation heuristics for inclusion in SMaRT.

2001-2002: Introduce the multidisciplinary project studio course for undergraduate seniors in which students will work in teams composed of management, computer science, accounting, and design majors collaborating as they design and develop electronic commerce systems for industrial partners.

III. INTEGRATING RESEARCH AND EDUCATIONAL EXPERIENCES

As previously mentioned, we will collect data on the analysis and design activities of projects in the studio. Specifically, we are interested in the role of goals and scenarios in constructing security and privacy policies and for operationalizing these policies into actual system requirements.

Goals are the objectives and targets of achievement for a system. Goal-driven requirements engineering approaches focus on why systems are constructed, expressing the rationale and justification for the proposed system. These justifications are sometimes embedded in policies and are often overlooked. Focusing on goals, instead of specific requirements, allows analysts to communicate with stakeholders using a language based on concepts with which they are both comfortable and familiar. Goals are operationalized and refined into requirements and point to new, previously unconsidered scenarios. Similarly, scenarios also help in the discovery of goals [AMP94, AP98, JBC98, Pot99, RSB98]. Although the merits and benefits of scenario-based and goal-based analysis in requirements engineering are well understood, researchers are now faced with the question of how to use scenarios and goals in a complimentary fashion. Several approaches do show promise [AAB99, MMM98, RSB98], but none address the integration of policy.

The Goal-Based Requirements Analysis Method (GBRAM) [Ant97] is useful for identifying and refining the goals that software systems must achieve, managing trade-offs among the goals, and converting them into operational requirements. The GBRAM is a straightforward methodical approach to identifying systems and enterprise goals and requirements. The method suggests goal identification and refinement strategies and

techniques through the inclusion of a set of heuristics, guidelines and recurring question types. These GBRAM heuristics and supporting inquiry [PTA94] include references to appropriate construction of scenarios and the process by which they should be discussed and analyzed. We have successfully applied this method to the analysis of systems for various organizations [AMP94, Ant96, Ant97, AP98, ADS00]. The latter two of these systems were electronic commerce applications [AP98, ADS00]. Students in the project studio will employ the GBRAM to support the early stages of the design process.

A. Scenario Management

The state of scenario management in practice was reported in [WPJ98]. In this study, the use of scenarios was examined in 15 European projects to learn how scenarios were produced and utilized as well as to identify the benefits and problems associated with scenario usage in industrial settings. As documented in [WPJ98], practitioners using scenarios and/or use cases in industrial settings incur very specific challenges. Specifically, Weidenhaupt et.al. highlight several key areas needing support including: the need for appropriate process guidance as well as comprehensive support for managing both scenario traceability and evolution.

Researchers at North Carolina State University (NCSU) are developing scenario management strategies [AAB99] in an effort to address the challenges discussed in [WPJ98]. The NCSU scenario management strategies support evolution by employing shared scenario elements to identify and maintain common episodes among scenarios. Measures are used to quantify the similarity between scenarios, serving as heuristics that provide process guidance to practitioners in finding, for example, duplicate scenarios, scenarios needing further elaboration or those that may have been previously overlooked.

We are currently developing a web-based tool (SMaRT) for analysts to quickly and easily enter scenario data; the tool will automatically check for redundancy and glossary term creation, requiring minimal time to examine other scenarios for consistency. The tool allows variability in redundancy checking, so tradeoffs can be made between consistency and the ease of use on an individual project basis. It can also identify similar scenarios and examine redundancy, consistency and coverage. Within the context of the project studio, the SMaRT will serve as an experimental research engine to support our empirical investigations, allowing us to further explore the role of scenarios and goals in ensuring coverage of security and privacy requirements in electronic commerce systems.

B. Domain Specific Goal Classes

The notion of reusable goal classes that occur in various types of software systems is discussed in [Ant97]. We are developing generalizable classes and subclasses of goals, which may be viable for more than one system, providing a way to carve up a problem domain. Problem domains may be decomposed into goals about process, security, etc. so that the classes dictate both what the system goals are and what they mean.

The goals for electronic commerce applications are classified according to subject matter, as reported in [AP98a]. These electronic commerce goal classes are:

- process support goals;
- electronic commerce goals;
- information display and organization goals; and
- security and access control goals.

Process support goals describe goals that pertain to system processes enacted by the user or the system. Electronic commerce goals deal with the base functionality of the system. Information display and organization goals describe the organization and presentation of information by the system. Finally, security and access control goals describe those goals involved in limiting access to authorized users [AP98a]. Based on the findings from our data collection, we will derive and construct an additional class for privacy goals.

These goal classes have been applied in the analysis of two electronic commerce systems [AP98, ADS00]. These studies demonstrate that the availability of goal classes can indeed be very beneficial when developing the requirements for systems since the goal classes can help ensure that all expected behaviors have been considered for the given system. A library of reusable goal

classes will be incorporated into the SMaRT and made available to project studio participants.

Our data collection during the electronic commerce design and development activities will enable us determine whether there are clusters of specific goal classes in a broad spectrum of electronic commerce systems. This determination will impact the heuristics in SMaRT by indicating refinements for the heuristics which call for the addition of specific questions for analysts to ask regarding goals which fall into particular goal classes.

IV. THE APPLICATION DOMAIN

Internet systems must be designed and developed with intrinsic security. The application domain of electronic commerce is especially suited for educating students due to the need to address the security and privacy which will enable future electronic commerce systems to be developed more securely and robustly without compromising individual privacy rights.

A. Electronic Commerce

Electronic commerce greatly reduces administrative costs and improves efficiency by enhancing customer responsiveness and speeding up product delivery time. However, protecting a digital marketplace is more complex than protecting the physical one. Information is dispersed so easily through electronic transactions that it is often difficult to differentiate between illegal actions and legitimate market research [ATW98, Bor96]. Concerns over the security and integrity of electronic commerce transactions initially stifled the adoption of e-commerce [Ale98, Ger97]; however, this is no longer a primary concern. Although Internet security is sometimes considered poor, it does not seem to be impeding the rapid growth of electronic commerce initiatives. Some businesses and individuals are willing to accept the risks; however, Internet users as a whole are concerned about their personal privacy and the security of their online transactions [CRA99]. The ability to ensure secure transactions is essential for businesses to be successful in the online commerce environment. The need to authenticate data and the identity of the sender, as well as the need to keep monetary and proprietary information secure is critical to the continued evolution and adoption of electronic commerce. Both business security and consumer confidence plays a significant role; hence the need for secure online transactions for both merchants and consumers. Students engaged in the project studio experience will receive hands-on experience with designing and developing such systems.

B. Privacy

Privacy is a concept that is not easily defined [Tav99], but it is often thought of as a moral or legal right [Cla99]. [Cla99] describes privacy as the "interest individuals have in sustaining personal space free from interference by other people and organizations." Information privacy is impacted by organizational functions such as electronic commerce, database management, security techniques, telecommunications, collaborative systems and systems implementation [EP99]. Developers of these systems need to be aware of this connection and realize the multidisciplinary approach necessary for successful e-commerce systems.

Smith et.al. explored the privacy concerns of consumers in a heterogeneous setting [SMB96]. They created an instrument for measuring individuals' concerns about organizational practices and identified a set of dimensions for principal privacy concerns: collection, unauthorized secondary use, improper access, and errors. Self-regulation has been proposed as a means to address concerns about consumer privacy [McG99]. The FTC recently issued a report to Congress encouraging industry to address consumer concerns about privacy through self-regulation [FTC98] despite the fact that self-regulation had previously been encouraged and most online businesses still had not adopted the fundamental fair information practices that address consumer privacy. In response, [Ben99] suggests the consideration of privacy seals (e.g. TRUSTe, BBBonline and WebTrust) to prevent the introduction of legislation that will be introduced if companies can not effectively achieve self-regulation. Alternatively, the P3P project (Platform for Privacy Practices Project) is being developed as a means to enable Internet users to exercise

preferences over Web site privacy practices [RC97]. Clearly, it is necessary to consider these factors throughout the requirements determination and software design of electronic commerce systems, as we seek to achieve during the studio project experiences.

C. Security

Strong security measures, including encryption, firewalls, policies and passwords, are needed to prevent the damage that results from unauthorized access to sensitive information (e.g., unauthorized destruction, modification or disclosure). The increase in computerized transactions and networked communications between organizations and consumers are the basis of technical safeguards playing a more important role in today's businesses. Transactions conveyed on paper are somewhat secure because of the inherent difficulty of accessing and searching their content, thus hindering their usefulness both to users and abusers who might breach confidentiality. When transactions are stored and exchanged in computerized information systems, however, they become more accessible. This creates the potential for wider and more systematic breaches of personal privacy. Computerized systems are also more vulnerable to accidental distortion, distribution and deletion of critical data [EPB00]. Successful privacy and data protection is a result of appropriate security measures and protecting an electronic commerce system cannot be accomplished with a single security method. Appropriate combinations of proven policies, procedures and devices will ensure the success of a secure networked environment.

Reducing threats to sensitive data is the focus of several studies addressing ways to physically provide better security for consumer privacy [BB95, MW98]. However, the balance between security and the information necessary for normal business operation must also be considered [EP00]. One approach to seeking this balance is proposed by [BB95]; they have introduced a method to de-personalize the data that is stored: systems require a file access table to reconstruct distributed bits of an individual's record. Thus, a disaggregated virtual record would replace the integrated personal file, thereby eliminating, or at a minimum reducing, any privacy concerns caused by using names and permanent identification numbers.

Most organizations are aware of the problem of unauthorized access to personal data, but few have established an effective security program for their systems [SKR99]. Although many organizations have developed a privacy policy for employees to follow; these policies provide no real guarantee against unauthorized access. Goal and scenario analysis, as prescribed in GBRAM and supported in SMaRT, offers a methodical and systematic approach to both formulating such policies and guaranteeing that a system's requirements are in compliance with these policies. Despite the increased awareness of heightened security needs, most organizations are facing a shortage of security skills [Mak99], highlighting the need for more research and education into security methods for electronic commerce.

Systems must be protected from both internal and external threats and their protection deserves special consideration during the early design stages. Typically, the formation of a security policy, discussed in the following subsection, is the initial aspect for consideration during the design of an electronic commerce system.

D. Policy

The primary step in securing an electronic commerce system is developing and implementing a dynamic document called a security policy [Dea00], which identifies the following aspects of the system:

- the security goals;
- risks;
- levels of authority;
- the designated security coordinator and team members;
- responsibilities for each team member and each employee;
- procedures for addressing security breaches; and
- other details impacting system security.

Although several methods for developing specific types of security policies have been proposed [AB95, Oln94, NI94, OA95, Lic97]; no innovative methods have been utilized to create policies specific to electronic commerce systems.

Knowledge of the business aspects of the system helps inform organizations about what needs to be protected. The ability to determine where the business need is for security and what security features are appropriate for the system is vital when developing electronic commerce applications for today's businesses.

A recent FTC report defines a privacy policy as a comprehensive description of a Web site's practices that is located in one place on the site and may be easily accessed [FTC98]. Every organization involved in electronic commerce transactions has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information and to take steps that foster the adoption and implementation of effective online privacy policies by the organizations with which they interact. Organizations engaged in electronic transactions should disclose a privacy policy that is based on fair information practices. The Georgetown Internet Privacy Policy Survey found that only 65.9% of these types of Web sites investigated in 1999 posted privacy disclosures [Cul99]. The study also found that the disclosures did not always reflect fair information practices. This implies the need for electronic commerce professionals to gain experience in developing proper privacy policies. We seek to equip our students with the skills and experience required for policy formation via our multidisciplinary approach to software engineering education.

V. EDUCATIONAL RESOURCES

We now discuss the educational resources that will be used in the studio as well as the educational resources that we will produce and disseminate broadly via the Internet to other electronic commerce and software engineering researchers and educators.

A. Incorporating Networking and Security Technologies in Development

Electronic commerce applications must be supported by the organization's network infrastructure; therefore, developers of such applications must have a great appreciation for and understanding of the capabilities and limitations of the infrastructure that supports the applications [Me99]. The project studio will address this by providing access to the current state of the art networking technology concepts. Furthermore, establishing suitable security and privacy policies for the electronic commerce applications requires the studio participants to also have a clear understanding of networking concepts. The Business Management participants will have encountered these basic concepts in a prerequisite course, however additional networking knowledge will need to be available to all studio participants. To this end, we expect to include the participation of graduate students enrolled in the new NCSU Computer Networking Master's degree program.

A suite of networking, as well as policy and software engineering, concepts will be available to the participants via "lectures on demand" and via project guides and instructional manuals. Details regarding the four networking standards architectures (TCP/IP, OSI, SNA, IPX/SPX) and various computing platforms will be available to assist the development team in successfully structuring their application and policies to consider the architectural standards.

A primary element of electronic commerce applications is the successful transmission of confidential data. For this to be successfully achieved, studio students will need a thorough understanding of all available security technologies. A collection of information concerning topics such as public key encryption, secret key encryption, digital signatures, digital certificates, digital watermarks, firewalls, and Secure Sockets Layer will be provided to studio participants. Access to such technical information will provide a foundation for developing successful electronic commerce applications with appropriate security measures incorporated to protect the system and users' privacy.

B. Software Engineering / Electronic Commerce Project Repository

As previously mentioned, the SMaRT will serve as a research engine, enabling us to collect data about research activities and processes. Additionally, SMaRT will be employed to support our educational mission. The tool will be an invaluable resource, given the project-based nature of the courses we teach and the project studio. Furthermore, it will be beneficial to

students, supporting their requirements activities and serving as a repository of example projects, scenarios, and requirements documents. The repository will be beneficial to instructors given that it will serve as a source of cases for future classes and as a source of real examples that may be used to demonstrate various software engineering principles.

VI. SUMMARY AND FUTURE WORK

A project studio is currently being developed to educate NCSU students about developing secure and reliable electronic commerce systems. The NCSU electronic commerce studio serves as a unique testbed for exploring and educating undergraduate students about the implications of internet security on the development of the next generation software applications. Specifically, we seek to provide increased visibility into the tasks and process of requirements engineering for evolutionary systems in which policy considerations play a major role. Our underlying research focuses on applying scenario management and goal-driven analysis strategies to facilitate the design and evolution of electronic commerce systems with a primary focus on security and customer privacy. Practitioners will profit from this initiative through a set of original development methods for software-based information systems in which security and privacy are imperative. Benefits for students will parallel as we provide them with exposure to the critical consideration of security and privacy in software systems. They will also gain real-world experience through participation in multidisciplinary development projects.

We expect students to benefit from increased exposure to a critical national need, security and privacy in software systems. Finally, we plan to develop a library of electronic commerce projects leading to new materials, such as techniques, methods and cases for undergraduate and graduate software engineering, information systems and electronic commerce education.

VII. ACKNOWLEDGEMENTS

The authors wish to thank Dr. Michael Rappa, NCSU College of Management Distinguished Professor and director of the NCSU Electronic Commerce Center, is assisting us in our efforts to secure industry support for this project studio.

REFERENCES

[AB95] M.D.Abrams and D.Bailey. Abstraction and Refinement of Layered Security Policy, *Information Security – and Integrated Collection of Essays* (Abrams, Jajodia and Podell, eds.), IEEE Computer Society Press, Los Alamitos, CA, 1995.

[ADS00] A.I. Antón, J.H. Dempster and D.F. Siege. Deriving Goals from a Use Case Based Requirements Specification for an Electronic Commerce System, *Submitted to the Sixth Intl. Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ)*, Stockholm, Sweden, June 5-6, 2000.

[Ale98] R. Alexander. Ecommerce Security: An Alternative Business Model, *Journal of Retail Banking Services*. (20)4, pp. 45-50, 1998.

[AAB99] Alspaugh, T.A., A.I. Antón, T. Barnes, and B. Mott. An Integrated Scenario Management Strategy, *International Syposium on Requirements Engineering (RE'99),* Limerick, Ireland, pp. 142-149, June 1999.

[AMP94] A.I. Antón, W.M. McCracken and C. Potts. Goal Decomposition and Scenario Analysis in Business Process Reengineering, *Advanced Information System Engineering: 6th Int'l. Conf., CAiSE '94 Proc.*, Utrecht, The Netherlands, 6-10 June 1994, pp. 94-104, 1994.

[Ant96] A.I. Antón. Goal-Based Requirements Analysis, *Second IEEE International Conference on Requirements Engineering (ICRE '96),* Colorado Springs, Colorado, pp. 136-144, 15-18 April 1996.

[Ant97] A.I. Antón. *Goal Identification and Refinement in the Specification of Software-Based Information Systems*, Ph.D. Dissertation, Georgia Institute of Technology, Atlanta, GA, 1997.

[AP98] A.I. Antón and C. Potts. The Use of Goals to Surface Requirements for Evolving Systems, in *Int'l. Conference on Software Engineering (ICSE '98),* Kyoto, Japan, pp. 157-166, 19-25 April 1998.

[ATW98] R.J. Alberts, A.M. Townsend and M.E. Whitman. The Threat of Long-arm Jurisdiction to Electronic Commerce, *Communications of the ACM*, 41(12), pp. 15-20, December 1998.

[BB95] V.M. Brannigan and Beier, B.R. (1995). Patient Privacy in the Era of Medical Computer Networks: A New Paradigm for a New Technology. *Medinfo*, 8 Pt 1: 640-643.

[Ben99] Paola Benessi TRUSTe: An Online Privacy Seal Program. *Communications of the ACM*. 42(2), pp.56 – 59. February 1999.

[Bor96] N.S. Borenstein. Perils and Pitfalls of Practical Cybercommerce, Communications of the ACM, 39(6), pp. 36-44, June 1996. [Cla99] R. Clarke. Internet privacy concerns confirm the case for intervention, *Communications of the ACM*, 42(2), pp. 60-67, February 1999.

[Cow98] A.J. Cowling. A Multi-Dimensional Model of

the Software Engineering Curriculum. *Proceedings of the 11th Conf. on Software Eng. Education & Training*, pp. 44-55, Atlanta, Georgia, 22-25 February 1998.

[CRA99] L.F. Cranor, J. Reagle and M.S. Ackerman. Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, *AT&T Labs-Research Technical Report TR 99.4.3*, April 1999.

[Cul99] M.J. Culnan, *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission*, http://www.msb.edu/faculty/culnanm/gippshome.html, Sun Microsystems White Paper on Security Policies, June 1999.

[Dea00] T. Dean. Network+: Guide to Networks, *Course Technology*, 2000.

[DJS96] P. Dart, L. Johnston, and C. Schmidt. Enhancing Project-Based Learning: Variations on Mentoring, *Proc. of the 1996 Australian Software Eng. Conf.*, pp. 112-117, 14-18 July 1996.

[DHH99] R.Dhamija, R.Heller and L.J.Hoffman. Teaching E-Commerce to a Multidisciplinary Class. *Communications of the ACM*, 42(9), pp.50-55, September 1999.

[EP99] J.B. Earp and F. C. Payton. Dirty Laundry: Privacy Issues for IT Professionals, *IT Professional*, March/April 2000.

[EP00] J.B. Earp and F. C. Payton. Information Privacy Concerns Facing Health Care Organizations in the New Millennium, *Submitted to Medical Informatics*, January 2000.

[EPB00] J.B. Earp, F.C. Payton and D. Baumer. Health Care Information Privacy: The Role of Law, Database, and Security Technologies. *Submitted to Computers and Society*, February, 2000.

[FTC98] *Privacy Online: A Report to Congress*, http://www.ftc.gov/reports/privacy3/, Federal Trade Commission, June 1998.

[Ger97] C. Germain. *Summary of the City University Security Survey 1997*, http://www.city.ac.uk/~eu687/ security/summary.html, 1997.

[JBC98] Jarke, M., X.T. Bui and J.M. Carroll. Scenario Management: An Interdisciplinary Approach *Requirements Engineering Journal*, Springer Verlag, 3(3-4), pp. 154-173, 1998.

[Lic97] S. Lichtenstein. Developing Internet Security Policy for Organizations. *Proc. of the 13th Hawaii Int'l. Conf. on System Sciences*, Vol 4, p. 350-357, 1997.

[Mak99] J.Makris. Firewall Services: More Bark than Bite. Data Comm. Int'l., 28(3), pp.36-50, March 1999.

[McG99] H. McGraw III. Online Privacy: Self-Regulate or Be Regulated, *IT Professional* (IEEE Computer Society), 1(2), pp. 18-19, 1999.

[Me99] D.G. Messerschmitt. *Networked Applications: A Guide to the New Computing Infrastructure*. Morgan Kaufman Publishers, Inc. San Francisco, CA, 1999.

[Me99] D.G. Messerschmitt. *Networked Applications: A Guide to the New Computing Infrastructure*. Morgan Kaufman Publishers, Inc. San Francisco, CA, 1999.

[MMM98] Maiden, N., S. Minocha, K. Manning and M. Ryan. CREWS-SAVRE: Systematic Scenario Generation and Use, *Int'l. Conf. on Requirements Engineering (ICRE'98),* pp. 148-155, April 1998.

[MW98] N. Memon and P.W.Wong. Protecting Digital Media Content, *Communications of the ACM*, 41(7), pp.35-43, Jul 1999.

[NI94] *Computer Securty Policy*, Computer Systems Laboratory Bulletin, 1994.

[OA95] I.M.Olson and M.D.Abrams, Information Security Policy, *Information Security – and Integrated Collection of Essays* (Abrams, Jajodia and Podell, eds.), IEEE Computer Society Press, 1995.

[Oln94] J. Olnes. Development of Security Policies, *Computers and Security*, 13(8), 1994.

[OM94] M.J. Oudshoorn and K.J. Maciunas. Experience with a Project-Based Approach to Teaching Software Engineering. *Software Education Conf. Proc.*, pp. 220-225, 22-25 November 1994.

[Pot99] Potts, C. A ScenIC: A Strategy for Inquiry-Driven Requirements Determination, *Proc. IEEE 4th Int'l. Symposium on Req'ts Eng.*, Ireland, 7-11 June 1999.

[PTA94] Potts, C., K. Takahashi, and A. Antón. Inquiry-Based Requirements Analysis, *IEEE Software*, 11(2), pp. 21-32, March 1994.

[RC97] J. Reagle and L. F. Cranor. The platform for Privacy Preferences. *Communications of the ACM*. Pp.48-55.Vol.42, No.2, Feb. 1997.

[RSB98] C. Rolland, C. Souveyet and C.B. Achour. Guiding Goal Modeling Using Scenarios, *IEEE Trans. on Software Eng.*, 24(12), pp. 1055-1071, Dec. 1998.

[SKR99] D. Steinauer, S. Katzke and S. Radack. Basic Intrusion Protection: The First Line of Defense, IT Professional (IEEE Computer Society), 1(1), pp. 43-48, 1999.[SM99] Shimeall, T.J. and J.J. McDermott. Software Security in an Internet World: An Executive Summary, *IEEE Software*, 16(4), July/August 1999, pp. 58-61.

[SM99] Shimeall, T.J. and J.J. McDermott. Software Security in an Internet World: An Executive Summary, *IEEE Software*, 16(4), July/August 1999, pp. 58-61.

[SMB96] H.J. Smith, S.J. Milberg and S.J. Burke. Information Privacy: Measuring Individuals' Concerns About Organizational Practices, *MIS Quarterly*, pp, 167-196, June 1996

[Tav99] H.T.Tavini. Informational Privacy, Data Mining, and the Internet. Ethics and Information Technology, 1(2), pp.137-45, 1999.[WM00] C.Wilder and M.K.McGee. Putting the "E" Back in Business. *InformationWeek*, 31 January 2000.

[WPJ98] Weidenhaupt, K., K. Pohl, M. Jarke and P. Haumer. Scenarios in System Development: Current Practice, *IEEE Software*, 15(2), March/April 1998.