A Multidisciplinary Project Studio: Designing Secure Electronic Commerce Systems

***Annie I. Antón**, Department of Computer Science, North Carolina State University*
aianton@eos.ncsu.edu
***Julia B. Earp**, Department of Business Management, North Carolina State University*
julia_earp@ncsu.edu

ABSTRACT

Multidisciplinary systems design experiences are available 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 graduate level are participating in the design of electronic commerce systems while applying software engineering principles in the NCSU electronic commerce project studio.

I. INTRODUCTION

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. We seek to increase the skills and qualifications of our graduates seeking careers in electronic commerce technology, specifically in developing secure electronic commerce systems. In the NCSU project studio, students use 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 [1, 2] highlight the immediate need to address key issues within the research community. Specific challenges for policy research [1] 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. [2], 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 have been addressing these challenges in the electronic commerce project studio since Spring 2001.

II. STUDIO DESCRIPTION

The studio was established so that students, possessing various educational backgrounds could 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 (e.g. wireless). We are increasing the scientific basis of software engineering by developing new, more appropriate software process models for the electronic commerce application domain. This effort is enabling us to advance the state of software engineering education via multidisciplinary entrepreneurial software development. Students are learning to employ more reliable processes to build secure software. The studio is increasing 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 is formalizing 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 included the construction of software process and project management educational materials and 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 has been to ensure tailorability of all guides and materials for future emerging technologies and all transaction-based information systems that require a secure foundation. The studio is informally serving 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 [3, 4]. In particular, [5] 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 [6].

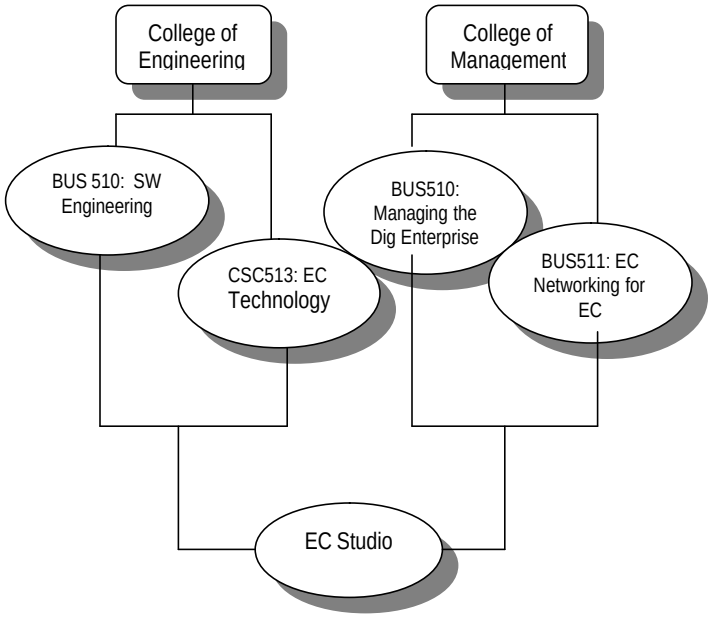

Figure 1: Curriculum Requirements for NCSU Electronic Commerce Project Studio

B. Prerequisites for Participation

The multidisciplinary nature of the project studio is intentional and is attracting students from various disciplines at NCSU. Each team of students, developing an electronic commerce system in the studio, includes representation from the NCSU College of Management and College of Engineering. These 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 complete two prerequisite courses: Managing the Digital Enterprise (BUS510) and Network Infrastructure for Electronic Commerce (BUS511). These students have knowledge regarding networking and security technologies, as well as the underlying managerial and privacy issues present in electronic commerce. College of Engineering students complete two prerequisite courses: Software Engineering (CSC510) and E-Commerce Technologies (CSC513). These students have advanced programming and software project management skills. While students from each of these majors have different skills and backgrounds, they each bring unique skills that collectively provide a student team with the broad range of skills and background necessary for a successful development team.

C. Studio Projects

Potential projects are solicited from the NCSU E-Commerce Corporate Sponsors[1] prior to each semester so that required software tools (such as Allaire Cold Fusion, IBM WebSphere, and other development and project management tools) may be obtained and installed prior to the first day of class. Final projects are selected based on their relevance to course objectives and educational value. The projects for the first two semesters were rather diverse and are briefly described in Table 1.

Company Name	Project Name	Project Description
Newton Instruments	Online Catalog	Entailed design and implementation of a prototype online catalog system for cable management. B2B/B2C.[2]
Newton Instruments	Order Tracking	Required specification, design and prototyping of an online user-friendly order tracking system. B2B/B2C.
Newton Instruments	GUI Design	Entailed re-engineering and design of company's Web site user interface. B2B/B2C.
Blue Cross Blue Shield of N.C.	Insurance Agent Quotation System	Enhancement and redesign of company B2B insurance agent Web site.
Haht Commerce	Knowledge Management	Involved the design of a knowledge sharing and sales tracking system for business and distribution partners.
Kodak	Online Bidding	Required specification, design and prototyping of an online bidding system.
Kodak	Non-standard Orders	Entailed design and implementation of a Web site to allow customers to place non-standard orders.
IBM	Inventing Workware	Involved specification and design of a communication technology to combine e-mail, instant messaging and online workrooms.
IBM	Napster for Consultants	Required specification, design and prototyping of a peer-to-peer system to address knowledge management issues.

Table 1: Project Descriptions

[1] The corporate sponsors are listed on the Studio Web site at http://ecommerce.ncsu.edu/studio/sponsors.html

[2] B2B refers to a Business to Business e-commerce system. B2C refers to a Business to Consumer e-commerce system.

III. INTEGRATING RESEARCH AND EDUCATIONAL EXPERIENCES

Student teams working in the project studio use a specialized process model intended to support e-commerce development. The process model employed during the first two semesters was the EPRAM (Evolutionary Prototyping with Risk Analysis and Mitigation) Model. Evolutionary prototyping, the foundation of the EPRAM model, is a form of software system creation in which developers gather the most complete, best-understood requirements possible, while designing and implementing a prototype for customer evaluation. This process is repeated until a working system emerges that encompasses the true set of customer and system requirements. The EPRAM model extends the traditional evolutionary prototyping approach by incorporating risk management as it pertains to e-commerce systems in particular, while imposing adherence to the Level 2 KPAs in the CMM [7]. The EPRAM process model consists of four development cycles. During the first cycle, some initial work is performed to establish the business case, plan the project, and better understand the customer's requirements for the desired system. The second cycle involves creating user interface prototypes for preliminary evaluation by the customer. During the third cycle customer feedback is incorporated into the first true working prototype. After subsequent customer evaluations, the prototype is again modified to address this additional customer feedback. Finally, the prototype is tested and delivered to the customer. Although the EPRAM Model proved very effective, the third semester is relying on an extension and refinement of the EPRAM model, ADAPT (Agile Development and Prototyping Technique).

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; therefore, we are collecting data on the analysis and design activities of projects in the studio. 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 [8, 9, 10, 11, 12]. 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 [13, 14, 12], but none address the integration of policy. The studio activities address this oversight by providing support for refining and extending the Goal-Based Requirements Analysis Method (GBRAM) [15] by developing heuristics to support security policy formation in the design of transaction-based information systems.

The GBRAM 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 [16] include references to appropriate construction of scenarios and the process by which they should be discussed and analyzed. Prior to offering the project studio, we had successfully applied this method to the analysis of systems for various organizations [8, 17, 15, 9, 18]. The latter two of these systems were electronic commerce applications [9, 18]. Students in the project studio now employ the GBRAM to support the early stages of the design process.

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 [19, 20]. Concerns over the security and integrity of electronic commerce transactions initially stifled the adoption of e-commerce [21, 22]; 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 [23]. 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 [24], but it is often thought of as a moral or legal right [25]. [25] 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 [26]. Developers of these systems need to be aware of this connection and realize the multidisciplinary approach necessary for successful e-commerce systems.

Self-regulation has been proposed as a means to address concerns about consumer privacy [27]. The FTC recently issued a report to Congress encouraging industry to address consumer concerns about privacy through self-regulation [28] 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, [29] 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) provides means to enable Internet users to exercise preferences over Web site privacy practices [30]. 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 [31]. 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 [32, 33]. However, the balance between security and the information necessary for normal business operation must also be considered [34].

Most organizations are aware of the problem of unauthorized access to personal data, but few have established an effective security program for their systems [35]. 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 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 [36], 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 [37], 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 [38, 39, 40, 41, 1]; 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 [28]. 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 [42]. The study also found that the disclosures did not always reflect fair information practices. Furthermore, these privacy policies fall short of truly safeguarding consumers [43]. This implies the need for electronic commerce professionals to gain experience in developing proper privacy policies. We equip our students with the skills and experience required for policy formation via our multidisciplinary approach to software engineering education.

V. SUMMARY AND FUTURE WORK

A project studio has been 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 graduate 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 goal-driven analysis strategies to facilitate the design and evolution of electronic commerce systems with a primary focus on security and customer privacy. Practitioners are beginning to 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 parallel as we provide them with exposure to the critical consideration of security and privacy in software systems. They also gain real-world experience through participation in multidisciplinary development projects. The students benefit from increased exposure to a critical national need, security and privacy in software systems. Finally, we are developing 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.

SMaRT (Scenario Management and Requirements Tool), a web-based tool that serves as an instrument to collect data on requirements engineering activities is currently under development at NCSU. It will soon be used in the E-Commerce studio and 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 in 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. ACKNOWLEDGEMENTS

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

REFERENCES

[1] S. Lichtenstein. Developing Internet Security Policy for Organizations. *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, Vol 4, p. 350-357, 1997.

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

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

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

[5] A.J. Cowling. A Multi-Dimensional Model of the Software Engineering Curriculum. *Proceedings of the 11th Conference on Software Engineering Education & Training*, pp. 44-55, Atlanta, Georgia, 22-25 February 1998.

[6] 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.

[7] M.C. Paulk. Using the Software CMM in Small Organizations, *Joint 1998 Proc. Pacific Northwest Software Quality Conf. and the Eighth Int'l. Conf. on Software Quality*, pp. 350-361, October 1998.

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

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

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

[11] C. Potts, ScenIC: A Strategy for Inquiry-Driven Requirements Determination, *Proceedings IEEE 4th International Symposium on Requirements Engineering (RE'99*), Limerick, Ireland, 7-11 June 1999.

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

[13] T.A. Alspaugh, 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.

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

[15] 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.

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

[17] 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.

[18] 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 International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ)*, Stockholm, Sweden, June 5-6, 2000.

[19] 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.

[20] N.S. Borenstein. Perils and Pitfalls of Practical Cybercommerce, Communications of the ACM, 39(6), pp. 36-44, June 1996.

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

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

[23] 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*, http://www.research.att.com/library/ trs/TRs/ 99/99.4/99.43/report.htm, April 1999.

[24] H.T.Tavini. Informational Privacy, Data Mining, and the Internet. Ethics and Information Technology, 1(2), pp.137-45, 1999.

[25] R. Clarke. Internet privacy concerns confirm the case for intervention, *Communications of the ACM*, 42(2), pp. 60-67, February 1999. [26] J.B. Earp and F. C. Payton. Dirty Laundry: Privacy Issues for IT Professionals, *IT Professional*, March/April 2000.

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

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

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

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

[31] 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.

[32] 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.

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

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

[35] 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.[2] 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.

[36] J.Makris. Firewall Services: More Bark than Bite. Data Communications International, 28(3), pp.36-50, March 1999.

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

[38] 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.

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

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

[41] 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, Los Alamitos, CA, 1995.

[42] 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.

[43] A.I. Antón, J.B. Earp, C. Potts and T.A. Alspaugh. The Role of Policy and Privacy Values in Requirements Engineering, *IEEE 5th International Symposium on Requirements Engineering (RE'01)*, Toronto, Canada, pp. 138-145, 27-31 August 2001.