Strategies for Developing Policies and Requirements for Secure Electronic Commerce Systems

Submitted to: 1st Workshop on Security and Privacy in E-Commerce at CCS2000
June 1, 2000

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

While the Internet is dramatically changing the way business is conducted, security and privacy issues are of deeper concern than ever before. A primary fault in evolutionary electronic commerce systems is the failure to adequately address security and privacy issues; therefore, security and privacy policies are either developed as an afterthought to the system or not at all. One reason for this failure is the difficulty in applying traditional software requirements engineering techniques to systems in which policy is continually changing due to the need to respond to the rapid introduction of new technologies which compromise those policies. Security and privacy should be major concerns from the onset, but practitioners need new systematic mechanisms for determining and assessing security and privacy. To provide this support, we employ scenario management and goal-driven analysis strategies to facilitate the design and evolution of electronic commerce systems. Risk and impact assessment is critical for ensuring that system requirements are aligned with an enterprise's security policy and privacy policy. Consequently, we tailor our goal-based approach by including a compliance activity to ensure that all policies are reflected in the actual system requirements. Our integrated strategy thus focuses on the initial specification of security policy and privacy policy and their operationalization into system requirements. 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.

1. Introduction

Organizations are hastily investing time and monetary resources in electronic commerce systems to support traditional business activities. By enhancing customer responsiveness and speeding up product delivery time, electronic commerce greatly reduces administrative costs and improves efficiency. 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 or flexible actions to accommodate electronic commerce partners [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 is not impeding the rapid growth of electronic commerce. Some businesses, as well as 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].

When compared to information systems of the past, electronic commerce systems are more vulnerable to accidental distortion, distribution and deletion of critical transaction data [EPB00]. Transactions conveyed on paper are somewhat secure because of the inherent difficulty of accessing and searching their content, thus hindering the usefulness to abusers who might breach confidentiality. When transactions are stored and exchanged using electronic commerce systems, however, information such as credit card numbers, electronic receipts and purchase orders become more accessible. This ease of access creates the potential for wider and more systematic breaches of information privacy. Information assets are core components of electronic commerce systems; therefore, protection of these assets is not an option but a necessity if commerce is to flourish.

Successful privacy and data protection is a result of appropriate security measures. Moreover, protecting an electronic commerce system cannot be accomplished with a single security method. It is important to identify appropriate combinations of proven policies, procedures and devices to ensure the success of a secure networked environment.

Although the Internet is a promising means of facilitating the growth of electronic commerce, there remain many 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 related to privacy and security pose a much greater challenge for researchers and software practitioners. To keep pace with the predicted explosive growth of electronic commerce, there is a great need for proven methods aimed at developing secure systems. This paper outlines an innovative approach for designing electronic commerce systems with a direct emphasis on addressing security and privacy needs from the early stages of conceptual design.

Our integrated approach applies goal and scenario-driven requirements engineering methods for secure electronic commerce systems resulting in the specification of: privacy policies, security policies and the corresponding system requirements for these proposed or envisioned systems. Section 2 provides an overview of the state of the research and practice in security and privacy policy. Section 3 provides relevant background in requirements engineering. Our strategy (an instantiated GBRAM model for policy development) is presented in Section 4, followed by a summary and discussion of future work in Section 5.

2. Security and Privacy

This section provides an overview of the relevant work in security, security policy, privacy and privacy policy.

Security

Reducing threats to sensitive data is the focus of several studies addressing methods to provide better security for data privacy [BB95, BS96, MW98]. However, the balance between security and information accessibility necessary for normal business operation must also be considered [EP00]. 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]. Electronic commerce systems must be protected from both internal and external threats and their protection deserves special consideration during the early design stages. Despite the increased awareness of heightened security needs, most organizations are facing a shortage of security skills [Mak99], highlighting the need for a heavier focus on systems with security requirements at the conceptual design phase. Similarly, Shimeall et.al. [SM99] highlight the increasing need for applications to be written with more concern for security to thwart the potential for vulnerabilities often exploited by attackers.

Although many organizations employ ethical codes for employees to follow; these policies provide no real guarantee against unauthorized access. The ability to determine where the business need is for security and what security features are appropriate, given the organizational environment, is vital when developing electronic commerce applications for today's businesses. The challenge lies in ensuring that the policies are reflected in the system requirements from which these electronic commerce applications will be designed.

Security Policy

The primary step in securing an electronic commerce system is developing and implementing a dynamic document called a security policy [Dea00], which identifies system aspects such as security goals and risks. It is important to establish who the authorized users might be, how they will access the system and data, how unauthorized users will be denied access, and how data will be protected within the organization as well as outside the organization.

Thoroughly planned security policies help minimize break-ins by communicating with and managing the users in an organization. Unfortunately, security policies are often treated as an after-thought [Trc00]. The strategies presented in this paper address this occurrence in electronic commerce systems by integrating policy creation and security considerations with requirements specification activities.

Although several methods for developing specific types of security policies have been proposed [AB95, And96, ISO98, Lic97, NI94, OA95, Oln94, PFI99, SW98, Trc00,]; few consider the dynamic nature and innovativeness of creating policies specific to electronic commerce applications [Oli97]. A security policy must address an organization's specific risks. To understand risks, an appropriate player should perform a security audit that identifies vulnerabilities and rates both the severity of each threat and its likelihood of occurring. Today's digital economy offers more areas for risk to be introduced through the involvement of various parties, such as suppliers, distributors, customers, and partners. Researchers [Lic97, SM99] highlight the immediate need to address key research issues in current security development methods. Specific challenges to policy research raised by Lichtenstein [Lic97] include the need to address the ill-defined content and structuring of content in policy development.

The PFIRES (Policy Framework for Interpreting Risk in eCommerce Security), developed at the Purdue University CERIAS (Center for Education and Research in Information Assurance and Security), provides a framework for managing information security policy for electronic commerce applications [PFI99]. The framework addresses the need to unify security policies in a manner consistent with organizational electronic commerce objectives. Security policies must be continually reviewed and updated to respond to changes in technology as well as the business environment; the PFIRES lifecycle model supports this iterative process by managing risks as an organization adopts new technologies which may compromise its existing security and/or privacy policies. While the PFIRES plan phase does include a requirements definition step, it does not currently offer systematic prescriptive guidance to the analysts who are actually responsible for translating policy recommendations into requirements.

Trcek [Trc00] has developed an approach to security policy management that provides an integrated solution from various fields (e.g. cryptography and human management). Trcek observes that development of information systems is typically top-down, whereas security methods are incorporated bottom-up; he thus advocates addressing policy development during analysis and design. His approach begins with an analysis of the business processes and identification of individual entities to be classified into security domains. Data flow diagrams are employed to model the process in a static perspective so that information flows may then be evaluated and enforced by flow controls. Trcek identifies some important aspects of policy management, but provides no guidance for the process of defining policy requirements.

Privacy

Privacy is a concept that is not easily defined [Tav99], but it is often thought of as a moral or legal right [Cla99]. Clarke describes privacy as the "interest individuals have in sustaining personal space free from interference by other people and organizations" [Cla99]. Privacy thus affects electronic commerce consumers as well as consumers, or stakeholders, in other domains. Consider, for example, the role of a patient's information privacy in the health care industry as explored in a recent study [EP00]. The study measured privacy perceptions of employees having daily exposure to information processing activities. The findings concluded that employees are torn between their respect for personal privacy and the need, whether imposed by management or through individual thinking, to collect personal information. Similarly, there exists a need to explore these same issues within the context of developing electronic commerce applications.

Self-regulation has been proposed as means to address concerns about consumer privacy [McG99]. The FTC (Federal Trade Commission) recently issued a report to the United States Congress encouraging industry to address consumer concerns about privacy through self-regulation [FTC98]. This report was presented 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 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) offers a means to enable Internet users to exercise preferences over Web site privacy practices [RC97].

Information privacy is impacted by organizational functions such as electronic commerce, database management, security techniques, telecommunications, collaborative systems and systems implementation [EP99]. Developers of electronic commerce systems need to be aware of this connection and realize the need for early privacy planning. Clearly, it is necessary to consider these factors throughout the requirements determination and software design of electronic commerce systems.

Privacy Policy

A privacy policy is defined as a comprehensive description of a Web site's practices which 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. Organizations also need to consider other organizations with which they interact and take steps that foster the adoption and implementation of effective online privacy policies by those organizations as well. Although, organizations engaged in electronic transactions should disclose a privacy policy that is based on fair information practices, the Georgetown Internet Privacy Policy Survey [GIP99] found that Internet privacy disclosures did not always reflect fair information practices. This highlights the need for electronic commerce professionals to gain experience in developing proper privacy policies and for practitioners to have access to prescriptive guidance for specifying the corresponding system requirements. The strategies presented in Section 4 include heuristics and techniques to aid practitioners as they develop both security and privacy policies which may be operationalized into system requirements.

3. The Role of Requirements Engineering in the Design of eCommerce Systems

Requirements engineering is the principled application of proven methods and tools to describe the behavior and constraints of a proposed system. As such, it arguably influences the outcome of a software project more than any other sub-discipline within software engineering [FB91] as well as the outcome of other analysis activities such as policy formation. Lichtenstein's framework for developing Internet security policy promotes a four phase strategy to engineer information security: requirements definition, design, integration, and certification or accreditation [Lic97]. Unfortunately, the framework offers no specific methods to address the requirements definition phase. Similarly, as previously mentioned, the PFIRES framework, does not provide adequate support for translating policy recommendations into system requirements [PFI99]. Although researchers in the requirements engineering community are beginning to focus on electronic commerce applications [AP98, ADS00, Rob97] there remains a need to apply proven requirements analysis methods (a routine activity in software engineering) and demonstrate how to best apply these methods within the context of establishing policy. Goal and scenario analysis have been successfully applied within the context of evolving electronic commerce systems [AP98] as we now discuss.

Goals and Scenarios

Goals are the objectives and targets of achievement for a system. In requirements engineering, goal-driven approaches focus on why systems are constructed, expressing the rationale and justification for the proposed system. Since goals are evolutionary, they provide a common language for analysts and stakeholders. 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. Furthermore, since goals are typically more stable than requirements [Ant97], they are a beneficial source for requirements derivation. Goals are operationalized and refined into requirements and point to new, previously unconsidered scenarios. Scenarios are descriptions of concrete system behaviors. They may summarize the behavior traces of an existing system. 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 for evolving systems in which risk and impact assessment as well as compliance become more paramount.

Goal-Based Requirements Engineering

The Goal-Based Requirements Analysis Method (GBRAM) [Ant96, Ant97, AP98, ADS00] is a straightforward methodical approach to identifying system and enterprise goals and requirements. It 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 method suggests goal identification and refinement strategies and techniques through the inclusion of a set of heuristics, guidelines and recurring question types. Four sets of heuristics are included: identification heuristics, classification heuristics, refinement heuristics, and elaboration heuristics. The heuristics are useful for identifying and analyzing specified goals and scenarios as well as for refining these goals and scenarios. The GBRAM heuristics and supporting inquiry 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].

Securing sensitive data is essential from the initial design phase of a system and the cost of security controls must be appropriate for the risk environment of the individual system. A risk analysis is needed to determine the stringency of the policy. This, in turn, will affect the cost of the security controls employed to meet the requirements of the security policy. Although methods and guidelines exist for managing and developing security policies [AB95, And96, ISO98, Lic97, NI94, OA95, Oln94, PFI99, SW98, Trc00], our goal-driven approach provides structured prescriptive guidance, in the form of a set of heuristics [Ant97, AP98, Dem00], for identifying new, previously overlooked goals based on the results of risk assessment activities. These goals are, in turn, operationalized into policies and system requirements.

4. Specification Strategies for Security Policy and Requirements

The primary goals in developing a security policy are to define organizational expectations for proper system use and define procedures to prevent, and respond to, security events. Similar to other organizational policies, the security policy must maintain and complement the organization's business objectives. The creation of a security policy for networked systems is inherently an ongoing and iterative process due to the dynamic nature of electronic commerce systems. When new technologies are adopted, an organization's security policy and privacy policy must be revisited and oftentimes revised to respond to the policy conflicts introduced by these new technologies. Thus, there is a need for an evolutionary approach for security policy development. Our proposed strategies involve the application of proven goal- and scenario-based requirements analysis techniques in the design and implementation of electronic commerce applications. The strategies and associated heuristics are designed to ensure that system requirements are in compliance with enterprise security and privacy policy.

The steps involved in security policy development for networked systems in general, include the following activities [Sun99]:

- identifying assets centered around software, hardware, people and documentation;
- evaluating and prioritizing those assets;
- identifying risks and vulnerabilities, including the probabilities of each;
- defining a policy of acceptable use based on work ethic and culture;
- identifying necessary safeguards, including physical security, audit/logging and incident response;
- creating the plan for a phased approach to introducing the policy; and
- communicating policy to users within the organization, as well as appropriate external individuals such as partners.

When applied specifically to electronic commerce systems, the risk identification phase is more significant and critical because such a highly interconnected environment inherently sustains added vulnerabilities. A risk occurs when a threat exploits a vulnerability to cause harm to the system. Security policies provide a baseline for implementing security controls to lessen risk introduced by vulnerabilities. The number of vulnerabilities in today's electronic commerce systems is massive when compared to the earlier environments of mainframes and dumb terminals. For this reason, system developers of the present require meticulous methods for organizing risk profiles into electronic commerce systems and system policy.

The strategies described below build on the PFIRES approach for assessing risk in eCommerce systems [PFI99]. The PFIRES framework employs a lifecycle model that consists of the following phases: Assessment, Planning, Delivery and Operation. While each phase of the model is marked by specific exit criteria that must be met before proceeding to the next phase, it does include feedback loops due to the iterative nature of policy development in eCommerce systems. Risk assessment is built into the lifecycle and policy changes are classified along a "change continuum"; *tactical changes* involve short-term goal achievement whereas *strategic changes* involve long-term, broad-based initiatives. Our strategy for policy formation focuses on goals that reside along this change continuum.

In requirements engineering, "strategic goals" are those that reflect high-level enterprise goals. Since these goals are typically more stable than requirements [Ant97], they are a beneficial source for requirements derivation. Similarly, one can safely assume that strategic goals are more stable, due to their long-term nature, than tactical goals. Both strategic and tactical goals are important, but as observed in previous studies, scenario analysis aids in ensuring that tactical (low-level) goals support an organization's strategic (high-level) goals [AMP94]. During goal analysis, analysts first explore any available information sources such as existing security and privacy policies, requirements specifications and design documentation to identify both strategic and tactical goals. These goals are documented and annotated with auxiliary information including the stakeholders and responsible agents. Goals are then organized according to goal type and arranged, according to their dependency relations, in a goal hierarchy. Detailed techniques and heuristics for each of these operations are described in [Ant97]. Once the goals are identified, they are elaborated. Goal elaboration entails analyzing each goal for the purpose of documenting goal obstacles, scenarios, constraints, preconditions, postconditions, questions and rationale. Goal refinement consists of removing synonymous and redundant goals, resolving any inconsistencies that exist within the goal set [Dem00], and operationalizing the goals into a requirements specification.

Figure 1 portrays the activities involved when instantiating the GBRAM for policy development. The rectangles represent information sources and/or artifacts whereas the ovals represent specific activities in which an analyst engages during the goal analysis process. The figure includes the traditional GBRAM activities (identify, elaborate, refine and operationalize goals) [Ant96, Ant97, AP98], but has been tailored for defining privacy policy and security policy. As previously mentioned, a critical step in policy formation is iterative risk assessment [PFI99, Sun99]. Risk assessment is thus introduced in this tailored version of the GBRAM; each goal is assessed for risks and potential impacts. As shown in Figure 1, risk identification may require one of two actions: goal refinement (e.g. by adding a constraint to mitigate the risk) or the addition of a new goal or sub-goal to respond to the risk. This is extremely important since system requirements in response to the adoption of new technologies, such as auctions [PFI99], may introduce a conflict with respect to the resulting policy. Heuristics, available in [Dem00], are applied to prevent such conflicts from being overlooked during the analysis process.

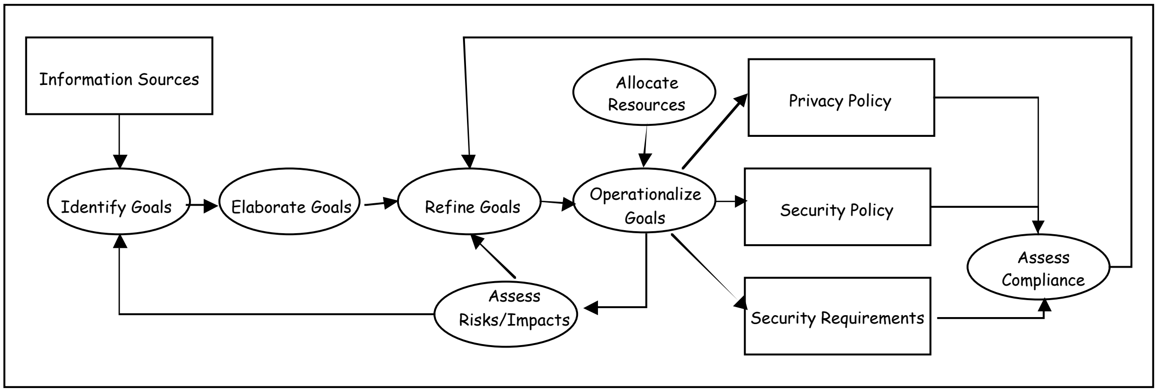

Figure 1: The GBRAM instantiated for Policy Formulation

In the GBRAM, goals are categorized in one of five goal classes: user, system, communication, knowledge and quality goals [Dem00]. *User goals* are associated with the actions performed by users while interacting with a given system. *System goals* involve processing actions or ongoing provision of services by the system. *Communication goals* describe the organization and presentation of information by the system as well as general system notification and messaging [AP98]. All communication goals are functional since they involve goal achievement. *Knowledge goals* are associated with information that should be known by the system or by the users. *Security goals* describe those goals involved in limiting access to authorized users [AP98]. Finally, *quality goals* describe the system, its data, or its processes in terms of standards or constraints. These categories are not mutually exclusive; that is, a particular goal can be, and often is, classified according to more than of these goal classes.

Our analyses of electronic commerce systems [AP98, ADS00] demonstrate that the availability of goal classes can 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. When goals are operationalized, we expect a correspondence between these goal classes and specific parts of the security policy as summarized in Table 1.

GBRAM Goal Classes [Dem00]	Common Security Policies [PFI99]
User Goals	User behavior policy
System Goals	Extranet/Internet policy Access to data policy Administration policy
Communication Goals	Administration policy
Security Goals	Password policy Remote access policy Extranet/Internet policy Incident response policy Security monitoring and audit policy Privacy policy
Knowledge Goals	User identification policy Access to data policy Incident response policy Awareness procedure pollicy Privacy policy
Quality Goals	Security monitoring and audit policy

Table 1: Security Policies and Corresponding Goal Classes

The goal classes we have identified to date [Ant97, AP98, ADS00, Dem00], do not address privacy. This is perhaps due to the tendency to focus on the system perspective. However, in our most recent electronic commerce case study, we distinguished between system and user goals due to increased consideration of the users' point of view. Privacy poses a special challenge since it is often the case that those who claim the biggest stake in a system are never really considered or involved in the design process as advocated by [BH98]. Thus, our strategy includes the participation of all representative stakeholders, including those who may not be obvious due to the nature of various systems in which privacy is critical.

We now demonstrate how scenario analysis and obstacle analysis aids analysts during goal-driven requirements engineering. Consider the following scenario for "Processing Membership Fees" from the CommerceNet web server case study [AP98]:

Actor	Action
User	find the membership application form
User	fill out membership application form
User	select e-check as payment method
User	type in public key
User	submit membership application form
Certification Authority	approve user payment
CN Server	respond to user with receipt
CN Server	increase budget balance
CN Server	create user's entry in member database
CN Server	add user to member mailing list
CN Server	add user to member web page
CN Server	send user membership kit

An event consists of an actor and an action [AAB99]. Each event in this scenario corresponds to a goal. As previously mentioned, goal and scenario analysis aides in elaborating and refining goals. For example, consider the obstacles and scenarios that correspond to the goal `MAKE payment method selected`, (event number 3 in the scenario above):

Goal	Obstacles	Scenarios
MAKE payment method selected	1. Payment method not selected 2. Payment methods not clear	1. User selects e-check as payment method 2. George isn't sure if Burdell & Assoc. has an account set up yet and needs to know to get one.

Obstacles #1 and 2 indicate the users' need to select from various payment options, such as check, money order, or credit card. Additional goals may be identified through the consideration of possible scenarios. For example, consider Scenario #2. George is an employee at Burdell & Associates. Before he selects a payment method, he must access his firm's CommerceNet Membership Web page to obtain the information he needs to select his firm's preferred payment method. This "walk through" approach has proven helpful in the identification of goals [AMP94, Ant96, AP98, PTA94].

Risk and impact assessment is necessary, but not sufficient for ensuring that system requirements are aligned with an enterprise's security policy and privacy policy. Consequently, an additional compliance activity is introduced. In software engineering, compliance is most commonly documented via requirements traceability [DP98, Ram98]. Traceability is a measure of quality that reduces the risk of, for example, not propagating changes across lifecycle artifacts. System documentation often remains unmodified after their initial creation and as a result often become obsolete [Ram98]. Our strategy ensures that a system's requirements specification, security policy and privacy policy are never obsolete by adopting an iterative compliance assessment activity, as shown in Figure 1. This final activity minimizes the risk of inconsistencies across the resulting requirements and policy artifacts by providing specific heuristics for identifying and mitigating any identified inconsistencies [Dem00]. The ultimate goal is to ensure compliance between the requirements specification and enterprise policies.

Consider an established enterprise preparing to introduce or unveil an electronic commerce system. The organization has existing policies that must be adhered to when developing the new system. The compliance assessment activity is demonstrated in Table 2, which follows the "House of Quality" (HoQ) [HC88] approach for documenting and analyzing large collections of requirements. The HoQ ensures that requirements reflect the enterprise policies, but requires the involvement of various stakeholders (customers, designers, marketing, etc.). The left hand column lists a set of enterprise policy statements whereas the top row lists a set of operationalized requirements, each in it's own column. The HoQ table indicates the relationships that exist among requirements and specific policies. A cooperating relationship is marked with a ✓ and a conflicting relationship is marked with an ✗ . When a conflicts arises between new goals and existing policies, the goal and/or policy are refined (as shown in Figure 1).

		Requirements		
Policy Statements		MAINTAIN member entrance to server	ENSURE content visibility to members only	MAINTAIN member data history (for user customization)
	Authentication is required for access to the commerce Web server.	✓	✓	
	All member account information will be kept confidential and used for internal business purposes only.			✗
	The firewall should be configured to limit data access to authorized member users.	✓	✓	

Table 2: Compliance Assessment Illustration

In our previous electronic commerce case studies (mentioned above) [AP98, ADS00], security policy and privacy policy were not at the forefront of our analysis, as was typical with those electronic commerce systems which were introduced during the first few years of web-based commerce. It is for this reason, that we are refining and extending the Goal-Based Requirements Analysis Method (GBRAM) by developing specific heuristics to support security policy and privacy policy formation in the design of transaction-based information systems as well as additional heuristics for operationalizing these policies into software requirements. Our preliminary activity process model for this extension, shown in Figure 1, will be validated within the context of the North Carolina State University eCommerce Systems Studio in which teams of graduate students design and develop eCommerce applications for industrial clients.

5. Summary and Future Work

Initially, corporate presence on the Internet was intended to provide 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 also engage in electronic transactions across the Internet, raising new security and privacy concerns. For privacy initiatives to succeed, they must be accompanied by tools and procedures that provide strong security [Cra99]. 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.

Our research seeks to demonstrate the viability and benefits of applying an goal-driven approach for ensuring security and privacy by addressing these concerns iteratively and during the early stages of the software design. We are developing heuristics to aid practitioners, policy strategists and system users in identifying and forming policies so they may be operationalized into requirements. These heuristics are based on goals and scenarios that provide a common language for all stakeholder communication. The proposed strategy is one of many approaches to designing security policies, however, it provides a more integrated approach based on work in the fields of requirements engineering and information security.

The goal and scenario analysis we are applying offers a methodical and systematic approach to both formulating policy goals and guaranteeing that a system's requirements are in compliance with these policies. Knowledge of the business aspects of the system helps inform organizations about what needs to be protected. The GBRAM has proven useful for gaining knowledge of such business aspects of systems as evidenced in two previous business process reengineering case studies [AMP94, Ant96].

The policy specification strategies and associated heuristics discussed in this paper are being developed and refined at the time of submission. An electronic commerce systems studio is being established as a means of supporting validation of this research. Industry sponsored projects will allow us to build case studies around the process of applying goal based approaches to electronic commerce systems. The studio will serve as a laboratory for designing such systems for industry use, while we continue to mature our strategies for managing electronic commerce policy and requirements. Studio participants will apply our strategies to various developmental situations, thus providing us with a collection of case studies to develop the necessary heuristics to validate the usefulness and efficacy of our methods. The studio projects will commence in August 2000 with participants involved in specifying security policy, privacy policy and system requiremetns for new, proposed or envisioned electronic commerce systems.

Acknowledgements

The authors wish to thank Michael Rappa for partial support of this work via the NCSU College of Management electronic commerce learning center and Gene Spafford for discussions that led to the formalization of the strategies presented herein.

References

[AAB99] T. Alspaugh, A.I. Antón, T. Barnes and B. Mott. An Integrated Scenario Management Strategy, *IEEE Fourth International Symposium on Requirements Engineering (RE'99),* University of Limerick, Ireland, pp. 142-149, 7-11 June 1999.

[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. Managing Use Cases During Goal-Driven Requirements Engineering: Challenges Encountered and Lessons Learned, *Submitted to IEEE 22nd International Conference on Software Engineering*, Limerick, Ireland, June 4-11, 2000. North Carolina State University Technical Report, TR-99-16, December 1, 1999.

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

[AMP94] 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.

[And96] R. Anderson. A Security Policy for Clinical Information Systems, *Proceedings of the 15 th IEEE Symposium on Security and Privacy*, 1996.

[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, *International 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] Brannigan, V.M. 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.

[BS96] B.Schneier, *Applied Cryptography : Protocols, Algorithms and Source Code in C* , 2nd ed. New York: Wiley, 1996.

[Cla99] R. Clarke. Internet privacy concerns confirm the case for intervention, *Communications of the ACM*, 42(2), pp. 60-67, February 1999.

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

[Cra99] L.F. Cranor. Internet privacy, *Communications of the ACM* 42(2), pp. 28-38, February 1999.

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

[Dem00] J.H. Dempster. *Iconsistency Identification and Resolution in Goal-Driven Requirements Analysis*, M.S. Thesis, North Carolina State University, Raleigh, NC, May 2000.

[DP98] Dömges, R., Pohl, K., Adapting Traceability Environments to Project-Specific Needs, *Communications of the ACM*, 41(12), pp. 54-62, December 1998.

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

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

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

[FB91] W.J. Fabrycky and B.S. Blanchard. *Life Cycle Cost and Economic Analysis*, Prentice-Hall, 1991.

[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.

[GIP99] Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission. Study Director Mary J. Culnan. http://www.msb.edu/faculty/culnanm/gippshome.html.

[HC88] J.R. Hauser and D. Clausing, The House of Quality, *Harvard Business Review*, 32(5), pp. 63-73, 1988.

[ISO98] Common Criteria for Information Technology Security Evaluation, ver 2.0, parts 1-3. ISO/IEC 15408, Geneva, May 1998.

[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. *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, Vol 4, p. 350-357, 1997.

[Mak99] J.Makris. Firewall Services: More Bark than Bite. Data Communications International, 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.

[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, Los Alamitos, CA, 1995.

[Oli97] R.W. Oliver. Corporate Policies for Electronic Commerce. Proceedings of the thirtieth Hawaii International Conference on Systems Sciences, pp.254-264, 1997.

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

[PFI99] Policy Framework for Interpreting Risk in eCommerce Security. CERIAS Technical Report, http://www.cerias.purdue.edu/techreports/public/PFIRES.pdf, Purdue University, 1999.

[Pot99] 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.

[Ram98] Ramesh, B. Factors Influencing Requirements Traceability Practice, *Communications of the ACM*, 41(12), pp. 37-44, December 1998.

[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.

[Rob97] W.N. Robinson. Electronic brokering for assisted contracting of software applets, *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, Volume: 4 , pp. 449-458, 1997.

[RSB98] 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.

[SKR99] D. Seinauer, 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.

[SP00] G.P.Schneider and J.T.Perry. *Electronic Commerce*. Course Technology, 2000.

[Sun99] Sun Microsystems. Protecting From Within : A Look at Intranet Security Policy and Management. http://www.sun.com/software/white-papers/wp-security-intranet/

[SW98] Straub, D. W. and R.J. Welke. Coping With Systems Risk : Security Planning Models for Management Decision Making." MIS Quarterly, vol. 2, no. 4, pp441-469. 1998.

[Tav99] H.T.Tavini. Informational Privacy, Data Mining, and the Internet. Ethics and Information Technology, 1(2), pp. 137-45, 1999.

[Trc00] D.Trcek. Security Policy Management for Networked Information Systems. *Proceedings of the Network Operations and Management Symposium, 2000*, pp. 817-830.

[Woo95] C.C. Wood. Writing InfoSec Policies. Computers and Society. Vol. 14, 1995.