Requirement Elicitation Based on Goals with Security and Privacy Policies in Electronic Commerce

Simara Rocha, Zair Abdelouahab & Eduardo Freire

Federal University of Maranhão, Electrical Engineering Department,
Av. dos Portugueses, S/N, CEP 65085-580, São Luís MA, Brasil
simararocha@uol.com.br, zair@dee.ufma.br, eduardo.freire@pop.com.br

Abstract

This paper describes a method for requirements elicitation based on goals for electronic commerce systems in agreement with security and privacy polices of the site. The method integrates the UWA approach [18] with the GBRAM method [3] for developing requirements policies for secure electronic commerce systems.

The resulting method has the objective to guarantee that existing security and privacy policies do not become obsolete with the adoption of new functionalities to a site. For this purpose, the method provides means so that requirements elicitation is in conformity with other ones.

In case organizations have not established its policies, the proposed approach suggests models through which it is possible the creation of such policies. The method still presents a model for requirements specification document in agreement with the approach described in this work. It seeks to establish a standard to specify software requirements to be useful for the development teams, in an attempt to facilitate the construction of systems, analyses, and for future maintenances or increment of functionalities to the site.

1. Introduction

In the elaboration and specification of software project, it is fundamental to observe and understand which requirements are necessary for that purpose. The quality of the product will depend strongly on a good capture and requirements specification. The goal is to determine not only what the software should do, but also the validation criteria, which will be used to evaluate what was previously defined.

However, to obtain the requirements is not always easy, because it involves a direct communication with the user and understands what the user wants. This is usually not a simple task. For this purpose, the use of appropriate techniques for that end can contribute in a significant way to optimize the process. For examples, the main objective in the development of a security policy is to establish the organizations expectations for a system and also the procedures to respond to security events.

Electronic commerce systems usually have dynamic nature; the creation of a security policy involves a progressive and iterative work [10]. When new technologies are adopted, the security and privacy policies must be reviewed and usually revised to respond to the conflicts introduced by these new technologies. Therefore, there is a need to devise approaches for the development and maintenance of security and privacy policies.

This work proposes the integration of the UWA approach [18] with the method GBRAM [3] instantiated for developing security policies with requirements.

2. Background

2.1. Approach UWA

In [9, 18, 19] the UWA (Ubiquitous Web Applications) project is presented. They describe a general framework whose purpose is to define a global technological and methodological umbrella

covering different aspects of the work to be carried out in a project of software.

The scope of the UWA project is the design of multi-device web applications. In particular, the aim is manifold: improving the quality of the design; improving the quality and effectiveness of the application; improving the process of design and improving the efficiency of the overall development-maintenance cycle; helping the developer to better cope with problems of evolution and changes of the application (dues to changes of context and/or changes of requirements).

UWA partitions the overall design problem in the following sub-problems or aspects of design as follows: definition of requirements -- establishing what the application must do; hypermedia design -- defining the information and interaction aspects of the application; operations design -- determining the operations that are made available to users by the application; transaction design -- establishing transactions of the application; and customization design -- defining the adaptation of the application to context features, and, in particular to the characteristics of the device, the connection channels, the location, etc.

The process guide for requirements elicitation in the approach UWA is composed by the following steps: stakeholder identification; elicitation of system goals; attachment of delivered values to goals; refinement of goals; documentation of assumptions, identification of the authorities; identification of risks associated with assumptions; identification of the operationalization criteria; identification of environment reification techniques; identification of requirement derivation techniques; application design and remaining steps are to measure and to validate the services given to users.

2.2.GBRAM Method Instantiated for Formulating Security Policies

In [2, 4, 5] the GBRAM method (goal-based requirements analysis) is proposed and in [3] the same method is instantiated for policy formulation, as it is illustrated by figure 1.

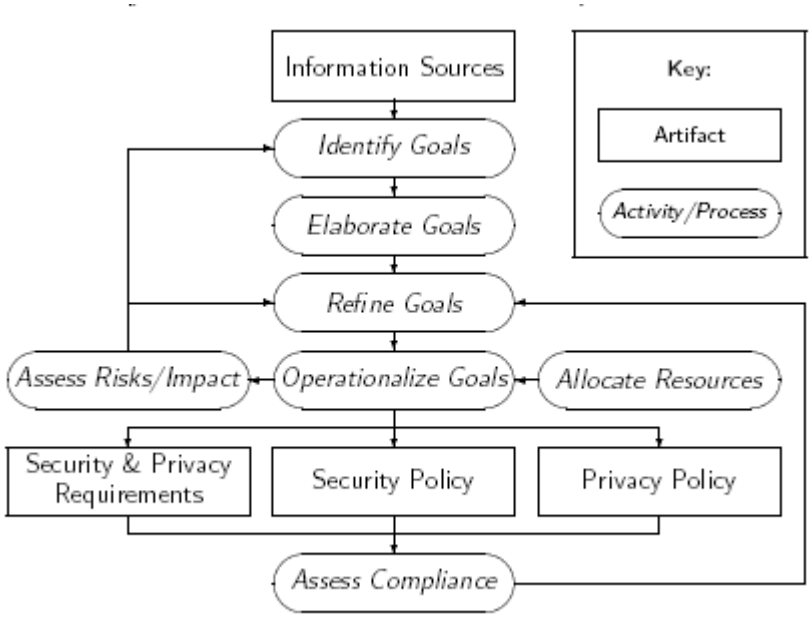

Figure 1 - GBRAM Security Policies

In the instantiated method, the same phases of the original GBRAM method maintained. However, some other phases are added such as: allocation of resources, assessment of risks and impacts and assessment compliance.

The phase of assessment of risks and impacts are based on PFIRES (Policy Framework for Interpreting Risk in e-Commerce Security) [15]. The PFIRES is a framework for interpretation of risks in security policy for electronic commerce, which uses a model of life cycle that consists of

the following phases: assessment, planning, delivery and operation. Each phase of the model is marked by specific exit criteria that must be met before proceeding to the next phase. Risk assessment is built into the lifecycle and policy changes are classified along a “change continuum”.

The phase of assessment compliance follows the HoQ (house of quality) [12], approach for documenting and analyzing large collections of requirements and it consists of a table, where the left column lists a set of enterprise policy statements whereas the top row lists a set of operationalized requirements, each in its 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 a “×”. When a conflict arises between new goals and/or existing policies, the goal and/or policy are refined (as shown in figure 1).

3. The Proposed Method

3.1. Phases of the Method

1 - Stakeholders Identification

If the Stakeholders are not adequately identified, characteristics of the system cannot be discovered, since they are the largest source of requirements of the system. For this reason, the method begins by the identification of the stakeholders.

The identification of the stakeholders can be realized starting from the exploration of existing documentation or through questions such as:" who or what has some interest in the system?", "who wins or loses with the development of the system?".

The method proposes that for each identified stakeholder it is necessary that the same is documented in the following way: number of the stakeholder, name and task that it executes.

2 - Elicitation of System Goals

This step consists of identifying requirements of the system in the form of goals (i.e. to express the goals or the desires that the stakeholders would like the system satisfy). This requires that each identified stakeholder establishes what the system should provide for the same perspective, letting the analysts of the system the coordination of those activities with the intention of extracting the largest possible number of goals.

In agreement with [16], a variety of techniques can be used to accomplish the task of capturing goals starting from the stakeholders. Among them, we can state: interviews, discussion groups and story-boarding.

To aid in the description of goals, the proposed method uses scenarios [6, 7, 8] for the detailed specification and also in the subsequent phase of operationalization.

3 - Attribution of Values to the Goals

In this phase, for each identified goal, the stakeholders responsible are asked the state of value they or the organization could obtain for the accomplishment of the goal. The value that a stakeholder gives to goals represents the benefit level that the goal will obtain when it is accomplished. Note that the value given to a goal is relative, since some goals can be more valuable for some stakeholders than others.

The method proposes that the attribution of values is done in the following way: collect all goals specified by the same stakeholder; enumerate in numeric scale ascendancy, in other words, the objectives are presented from the smallest to the largest value. The importance of attribution of a value to each defined goal will be particularly useful, particularly for resolutions of conflicts and refinement of goals.

Finally, after attributing a value to each goal, it is necessary that the same ones are ordered with respect to a dependency relationship that may exit among them. A dependency relationship specifies that a goal depends on the other in order to be accomplished. The method maintains the relationships of dependencies found within GBRAM [2].

4 – Refining Goals

After establishing values to each goal and stating their dependency relationships, the phase of goals refinement begins. This phase consists of a manual process accomplished by the analyst with the purpose of identifying inconsistencies, redundancies, unify synonyms and eliminate duplicated goals.

This step is necessary because the identified goals initially tend to be general and high-level. For this reason, the goals need to be refined in a more detailed and concrete forms so that they could be operationalized or accomplished.

It is important to point out that, in case a stakeholder has attributed the same value for two or more goals, the analyst should return to the previous step and ask the stakeholder to establish new values; thus guaranteeing the resolution of conflicts.

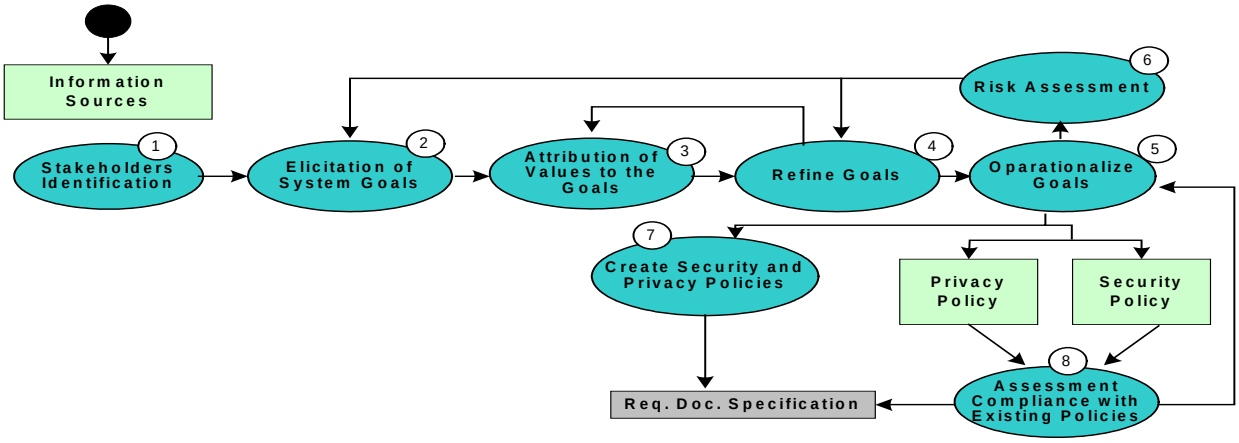

Figure 2 - The Proposed Method

5 – Oparationalizing Goals

After refining the goals, it is necessary that these ones are translated in terms of requirements; in other words, specifying the objectives (low level) that the system should accomplish to satisfy the goals. The translation consists of describing each goal in details in terms of scenarios within a template.

The proposed method uses an informal style to achieve this phase in a similar fashion as in GBRAM [1, 14], where a schema driven strategy is used, which is based on goal-schema, use-case-schema and scenario-schema. However, some adaptations are made and described below.

The first schema is the schema-goal whose purpose is to specify the relationships between goals and scenarios; a model of goals is specified for incorporating all information acquired in the previous phases. The syntax of the schema for the goal model consists of: the goal number, goal name, its description, stakeholder, value, code of scenario, pre-conditions and pos-conditions.

A schema is also used to specify scenarios and actions; the syntax of the schema consists of: a code of the scenario, a description, actor/agent, pre-condition and/or pos-condition and action.

Finally, the action schema is also used as form of specifying each action of a scenario; it is necessary at least one action schema for each scenario. However, each scenario may have several action schemas; the syntax of each schema consists of: action, type, entrance, sequence number and code of the scenario.

6 – Risk Assessment

According to figure 3, this phase is subdivided in three sub phases: identifying threats and vulnerability, estimating the occurrence probability and choosing a strategy of mitigation of risks. The proposed method uses some techniques contained in [11, 13], especially in the first and second sub phase. However some adaptations are made and explained below.

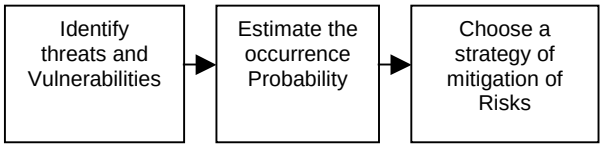

Figure 3 - Risk Assessment Sub Phases

The sub phase `*identify threats and vulnerability*' begins with the identification of pairs (threat, vulnerability) and also the threat-sources, motivation and actions that may result in an attack.

The sub phase `*estimate the probability of occurrence of risks*' is similar to [11], where the probability of occurrence of the risk is classified in three levels: high -- when the threat-source is highly motivated and sufficiently capable, and the controls to prevent the vulnerability are ineffective; medium -- when the threat-source is motivated and capable, but controls in place may impede successful exercise of the vulnerability; and low -- when the threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Finally, the sub phase `*choose a strategy of mitigation of risks*' consist of one of the actions, illustrated in figure 2: adding a new goal or sub-goal to respond to the risk, or a new goal refinement seeking to add a restriction for attenuation of the same one.

At the end of this phase, the proposed method can proceed in two ways: create security and privacy policy in case the organization has not defined yet its policies or assess compliance in order to guarantee that the requirements of the system are in agreement with existing security and privacy policies of the organization. Below, the two ways are explained.

7 – Create security and privacy policies

This phase consists of establishing a security and privacy policies for the organization site. The proposed method includes this stage as a form of guaranteeing that such policies are created. However, organizations with established security and privacy policies, the execution of this phase is unnecessary.

Header
<Title>
<Author (s)>
<Dates of the version >
< Number of the version >

1. Introduction
1.1. Statement on purpose
2. Policies
2.1. Identification and Authentication Policy
2.2. Encryption Policy
2.3. Awareness and Education Policy
2.4. Password Policy
2.5. Appropriate Use Policy
3. Appendix
3.1. Glossary
3.2. Related Documents

Figure 4 - Security Policy Template

For the conduction of this phase, the method suggests the adoption of models as form of establishing a standard middle (form) to build policies in a clearer way, less ambiguous and containing just the most important aspects benefiting the users of an electronic commerce site.

Figure 4 presents a template suggested by the method for the creation of a security policy for an electronic commerce site. Below all the items of the model are detailed.

The first part of the template is formed by a header, which is composed of a title of the document, name(s) of author(s), dates and version number of the security policy.

The next section of the template refers to an *introduction* which states the purpose of the policy (a brief description of why security policy is necessary and important for the site).

Soon after, the section Policies is shown and it is divided into five sub sections: *identification and authentication policy* which specifies the form the user should be identified and which restricted access they have and also the way the site will authenticate and validate the information supplied by users; *encryption policy* describes the technology type used by the site for encryption of information supplied by users; a*wareness and education policy* which establishes the form used by the site for communicating with customers and the types of electronic correspondences they can receive; *password policy* which is reserved for the site to show its users the best way for creating a password and the importance of the constant changes of the same one; *appropriate use policy* which contains a detailed description site usage rules as well as the responsibilities attributed to a user and its relationship with the organization.

The final section, a*ppendix* is constituted of two subsections: g*lossary* which is used to make any definition or explanation that can help reading and understanding security policy; and *related documents* where should be listed all the links with important information that can be useful to complement security policy.

Figure 5 presents a template suggested by the method for the creation of a privacy policy for an electronic commerce site. Its objective is to describe the types of information collected by the website and how these are manipulated, stored and used.

Header
<Title>
<Author (s)>
<Dates of the version >
< Number of the version >

1. Introduction
1.1. Statement on purpose
2. Principles
2.1. Notice/Awareness
2.2. Choice/Consent
2.3. Integrity/Security
2.4. Access/Participation
3. Appendix
3.1. Glossary
3.2. Related Documents

Figure 5 – Privacy Policy Template

Similar to security template, the privacy template also begins with a header followed by an *introduction* section which contains a statement and its purpose.

The following section contains various items such as: *notice/awareness* that specifies in detail all information collected about the user, how this information is stored and used by the site; *choice/consent* contains a description of the practices of the site allowing the user to choose to accept or not things that are established, for instance, download files or software, the completion of

forms of research purposes…etc; *integrity/security* which describes means used by the site to preserve and guarantee that the supplied data are not accessed, altered, modified or extinguished by non authorized individuals; *access/participation* which establishes ways users can access the colleted information, make the corresponding additions and corrections ...etc.

The last section, *appendix* is similar to the one of security policy and it consists of two subsections: glossary and related documents.

8 – Assessment Compliance with Existing Policies

According to figure 6 this phase is subdivided in three sub phases: assessing existing policies, identifying compliance and contradictions and developing an action strategy.

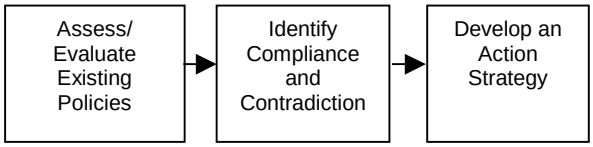

Figure 6 – Assessment Compliance Sub Phases

The sub phase '*evaluating existing polices'* is one of the most difficult and slow task, mainly if this is the first time the method is executed. However, this is indispensable that the sub phase is accomplished to give continuity to the process. The strategy proposed to lead the sub phase is based on HoQ [12].

Header
<Title>
<Author (s)>
<Dates of the version >
< Number of the version >

1. Introduction
1.1. Document Objective
1.2. Mark of the Product
1.3. General Vision of the Document
2. General Description
2.1. Functions of the product
2.2. General Restrictions
2.3. Postponed Requirements
3. General characteristics
3.1. Stakeholders Documentation
3.2. Goals Documentation
3.3. Documentation of the relationships of dependences among the goals
4. Schemas
4.1. Schema-objective
4.2. Schema-scenario
4.3. Schema-action
5. References
6. Appendix
5.1. Glossary
5.2. Other information

Figure 7 – Requirements Specification Document

With this strategy, the policies are examined extracting the declarations of policies of the site

and filling the column of the equivalent table of the examined policies for subsequent assessment compliance. For organization effect, it is important that security and privacy policies are analyzed separately. Soon after, starting from the specified requirements, the column of the elicited requirements is filled conform to HoQ.

After filling the table, the sub phase *'identifying compliance and contradictions'* begins and consists of establishing the existing relationships between the requirements and the policies of the site. The table is examined and filled out in agreement with the relationship found, where a compliance relationship is marked "✓" and a conflict with a "×".

Finally, the accomplishment of the sub phase '*develop an action strategy'* as illustrated in figure 2, depends on the relationship type found in the table; it can follow one of the two ways: returning to the phase of goal refinement is necessary whenever a requirement of an goal conflicts or is redundant with the existing policies; and the updating of the existing policies whenever these ones do not satisfy the specified requirements.

Finally, the proposed method suggests the adoption of a template for requirements specification document (figure 7) whose objective is to supply a middle-pattern to specify the elicited requirements [17]. For space reasons, we omit details of the specification document.

4. Comparative Study

Both approaches (UWA and the proposed) are based on goals (objectives that stakeholders would like the system satisfy) and requirements (low level objectives that the system supposedly should know and can be understood directly and accomplished by the planners). Other common aspect is that the two approaches are centered in the stakeholder identification.

Besides the phase of identification of stakeholders, two other phases are common to the two approaches, attribution of values to the goals and goals refinement. However, in the proposed method the phases involve a set of techniques and strategies that help to lead and to formalize the process of requirements elicitation. In UWA, such stages are executed in an informal way, in other words, there are no established or formalized strategies that help to the conduction of the stages.

The proposed approach maintains the dependency relationships contained in [2] GBRAM, as a form of ordering the goals. Another similarity with GBRAM is the phase of goal refinement, where synonymous goals are unified and the redundant ones are eliminated. The phase of operationalization of goals is also common to the two approaches. Although they use a similar type of extended template, the proposed method makes some adaptations to satisfy electronic commerce applications nature.

An important difference among those two approaches (GBRAM and the proposed) is that second is centered in the identification of the stakeholders, for believing that they are natural sources for deriving goals and not the opposite.

The instantiated GBRAM method for developing security policies is based on risk assessment, allocate resources and assess compliance. The risk assessment and compliance assessment phases were maintained in the proposed method. However, while the instantiated GBRAM method uses PFIRES, the proposed method uses patterns proposed by [15], as they are quite used by most sites of electronic commerce.

The proposed method still differs from the instantiated GBRAM, for possessing a phase of creation of a security policy and a privacy policy, adopting a template that seeks to establish them in clearer way, less ambiguous and containing just the most important aspects, benefiting the organization and users of an electronic commerce site.

Finally, the proposed method provides a template for requirements specification document as a form of establishing a standard middle to specify software requirements and provide a larger formalism to the created method.

5. Case Study

Seeking a verification and a validation of the proposed method, we have chosen to apply it in bookstore domain, to illustrate the applicability of all its phases. For lack of space, we present only

the most important aspects.

Using the strategies contained in phase 1 of the method, we have identified the following stakeholders: S1: Customer; S2: Employee of the bookstore; S3: Supplier; S4: Manager and S5: Distributor.

Using the techniques contained in phase 2, we have identified the following goals from the stakeholders: G1 - Register customer; G2 - Authenticate users; G3 - Accomplish purchases; G4 - Choose forms of payments; G5 - devolution of products; G6 - Choose address of request delivery; G7 - Exhibit a list of products which are mostly sold; G8 - Register products; G9 - Accompany accomplished requests; G10 - Send email at the end of each phase of a request, etc.

Still in phase 2, each objective should be operationalised using scenarios. Note that the scenarios should describe normal, exeptional, and variational behaviour.

In phase 3 it is attributed values to goals for the stakeholders. For example, the goals G1, G3, G4, G5 and G6 specified by stakeholder S1 would have respectively the following values: 1, 5, 3, 4 and 2. We also establish the following relationships of precedence dependency: G1 <G3 <G5.

Phase 4 is not applied because the goals within the example does not present redundancy, nor inconsistency nor duplication

Phase 5 illustrates the goals and scenarios schemas:

- Goal-schema
Goal Number: G1
Name: register Customer
Description: It consists registering the customer information for accessing restricted area of the site
Stakeholder: S1
Value: 1
Scenarios: C1
- Scenario-schema
Code of the scenario: C1
Description: register customer in a normal way
Actor/agent: Customer
Pré-conditions: If the customer data informed is valid
Pós- conditions: Do registered customer
Action:

1. The customer enters in the register area
2. The customer informs its personal data, username user and password for accessing the system
3. The system makes the validation of the content of the fields
4. The system stores the information in the data base
5. The system emits a message "registered with success"

- Action-schema
Action: The system makes validation of the informed data
Type: System
Entrance: Name, address, user and access password
Sequence number: 1
Code of the scenario: C1

Phase 6 makes risk assessment and can be evidenced by table 1.

Table 1. Example of phase 6

Treat	Vulnerability	Threat-Source	Threat Action	Probalbility	Srategy
cookies theft	✓ Cookies containing information without cryptography	Hacker, Cracker	✓Scripts injection on the customer's side ✓Use of Eavesdropping	High	✓Usage of SSL for making cryptography of all traffic

Analyzing the elicited goals and using the models presented in the phase 7, we have a sketch of security and privacy policies which will be completed only after the conclusion of the phase assessment compliance:

Privacy Policy
Simara Rocha
27/03/2005
Version: 1

1. Introcution

1.1. Statement on purpose

The bookstore Vinícius of Moraes has total commitment with respect to customer satisfaction during the whole the purchase process.

To demonstrate our commitment, we have opened this space for you customer, to show our conduct with respect to confidentiality of peoples information.

2. Principles

2.1. Notice/Awareness

The bookstore Vinícius of Moraes collects your personal data for the following purposes: register purchases, register our promotions, for conducting research and statistics, receive innovations of the site by email.

Your supplied personal information will not be, in any hypothesis, changed or marketed. Such information will be, however, to generate statistics and for better understanding the consumer profile.

2.2. Choice/Consent

Emails greeting, participation of promotions or research, as well as downloads of files or softwares will always be conditioned to customers consent, and will be informed in a clear way its aims, and the purpose of each one. Note that such authorizations can be revoked, at any moment.

2.3. Integrity/Security

To protect your information of any violations, the bookstore Vinícius of Moraes uses SSL. This software allows codify all your personal information, including credit card, turning it impossible for somebody to access this information in the net.

2.4. Access/Participation

At any moment our customers can access their information in Vinícius of Moraes, by just informing the user and the password to proceed with any modification.

Figure 8 - The Sketch of Privacy Policy

Analyzing the sketch of privacy policy described above, as well as the elicited requirements we proceed to phase 8 (Assessment compliance):

Table 2. Assessment Compliance

Privacy Policy Statements		REQUERIMENTS		
		Visible personal data only to the users profile	Suspend access after 3 attempts	Maintain just personal data stored
	Validation is requested to access restricted pages of the site	✓	✓	
	Collects customer data for purchase			×

As it is illustrated in the table above, the declaration "collects customers data for purchase" conflicts with the requirement "maintain just personal data stored". This means that we need to update the privacy policy. For example, the credit card number is not stored, it is only used at the moment of purchase.

The rest of this application cannot be completed in this paper for space reasons.

6. Conclusion

This work has the objective of studying some approaches based on goals and presents a method for Requirements Engineering for electronic commerce systems in obedience with existing security policy and privacy policy of a site. The main focus is to guarantee that such policies do not become obsolete for the adoption of new functionalities to the site. In this way, when new technologies or functionalities are adopted, the elicitation of requirements must be done in conformity with others. Another important aspect provided by our approach is the ability to create models for new policies, in case the site does not have defined its policies. The method also provides a template for requirements elicitation specification which can contribute to the agility and documentation of the process.

Our approach is originated from the integration of the approach UWA [18] with the method GBRAM [3] instantiated for developing policies and requirements for secure electronic commerce systems.

As future works, the extension of our approach with the phase of validation of goals together with requirements specification document is important. Another suggestion is the development of patterns for the proposed templates, which can help with the formalization of the method.

7. References

[1] A.I. Anton, 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.

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

[3] A.I. Anton, J. B. Earp, "Strategies for Developing Policies and Requirements for Secure Eletronic Commerce System", 1º Workshop on Security and Privacy in E-Commerce at CCS2000, November 2000.

[4] A.I. Anton 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.

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

[6] C.B. Achour, T. Mustapha, C. Souveyet, "Bridging the gap between users and requirements engineering: the scenario-based approach". Computer Systems Science and Engineering, v14, n6, Nov, 1999, p 379-388.

[7] C.B. Achour, C. Rolland, C. Souveyet, "A proposal for improving the quality of scenario collections". Proceedings of the Fouth International Workshop on Requirements Engineering: Foundations of Software Quality, REFSQ´98, Pisa, Italy Presses (eds, E. Dubois, A. L. Opdhal, K. Pohl), pp. 29-42, 1998.

[8] 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.

[9] D. Bolchini, P. Paolini, "Capturing Web Application Requirements through Goal-Oriented Analysis". WER, pp. 17-28, 2002.

[10] D. Bolchini, A.I. Antón and W. Stufflebeam, "I need it now: Improving Website Usability By Contextualizing Privacy Policies", To appear: The 4th International Conference on Web Engineering (ICWE 2004), Munich, Germany, 28-30 July 2004.

[11] G. Stoneburner, A. Goguen and A. Feringa. "Risk Management Guide for Information Technology Systems", NIST Special Publication 800-30, July 2002.

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

[13] J. Jaisingh and J. Rees. "Value at Risk: A Metodology for Information Security Risk Assessment", Purdue University, West Lafayette, IN, 2000.

[14] M. Carvalho e Z. Abdelouahab, "Um Método para Elicitação e Modelagem de Requisitos baseado em Objetivos", WER, 2001.

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

[16] R. Pressman, "Engenharia de Softwares". 3ª ed., São Paulo: Ed. Makron Books do Brasil Ltda., 1995. 1056p.

[17] S. V. Rocha, "Um Modelo para o Documento de Especificação de Requisitos baseado no Processo Unificado/UML", Monografia de Conclusão de Curso, MA, 2001.

[18] UWA Consortium, Requirements and Design Specification for Banca 121 Pilot Application, UWA Project Deliverable D11, available at www.uwaproject.org, 2001.

[19] UWA Consortium, Evaluation of UWA Design Methodology, UWA Project Deliverable D13, available at www.uwaproject.org, 2001.