Security and Privacy Requirements Analysis Tool (SPRAT)

Software Requirements Specification

Version 2.00
12, July 2004

Document Authors	Project Team	Team Role
Neha Jain (Main)	Dr. Annie I. Antón	Project Manager
Dr. Annie I. Antón	Qingfeng He	PGMT Developer
Qingfeng He	Neha Jain	Project Manager
William Stufflebeam	William Stufflebeam	SMaRT Developer
Jack Frink		

Project Sponsor
Dr. Annie I. Antón

Table of Contents

1. Introduction

Privacy and security policies for web-based systems are often developed as an afterthought. The implications are significant because the systems' requirements, policies and functionality are often misaligned and/or in conflict with each other. Organizations risk customer mistrust based upon customer perceptions of conflicting privacy statements. The identification of high-level goals is fundamental to requirements analysis specification process. This can be achieved by asking 'why' questions about the operational descriptions of the system available. Goals are important in the requirements engineering process because they bring completeness and ease of readability to the requirements. They also provide rationale for requirements and help detect conflicts. On the other hand, scenarios are used to specify desired behavior of the system and are the means of communication among stakeholders. Additionally, they support trade-offs amongst design alternatives. Based on the utility of goals and scenarios, there is a need to develop a tool, which will assist analysts in the scenario and goal *mining, reconciliation* and *management* processes. The tool aims to maintain a goal and scenario repository for use in continuing analyses of policies and other documents from which goals and scenarios can be derived.

All goals are fully traceable to the policies in which they are stated and are distinguished as either *policy goals* (strategic goals) or *scenario goals* (tactical goals) in each policy. This tool will provide strong management, which will offer flexible user defined conditions (like ID, keywords, taxonomy, subject, actor, and occurrences). The tool will also support automatic multi-user analysis results comparison. For example, each analyst can classify goals separately and the tool can automatically check the differences in their classification results for their resolution. Requirements engineers, Chief Privacy Officers (CPO), policy analysts or auditors will be able to use this tool. This document specifies the services that the tool will provide and the constraints under which the system must operate. It contains the following sections:

Description of Modules: This section contains a detailed description of the contents of each module.
FR: Functional Requirements: This section specifies the operational services that the tool will provide to its users.
NFR: Non-Functional Requirements: This section specifies the properties like accuracy, performance etc. that the tool must satisfy.
SPR: Security and Privacy Requirements: This section specifies security and privacy related requirements that ensure security of all sensitive data.
Requirements Traceability Matrix: This section graphically displays requirements dependencies.
Document Revision History: This section outlines the version of the current document being used, the people responsible for the document, dates the document is modified and the changes made to the document.
Appendix: This section contains a glossary of the terms used throughout this document. Additionally, it contains a bibliography of the references used in this document.

2. Module Breakdown

The SPRAT will be comprised of 6 main modules:

- **User Access Module** – This module manages access levels and permissions for each class of user. The included access levels are:
  a. *Administrator*
  b. *Project Manager*
  c. *Analysts*
  d. *Guest*
- **Goal Specification and Management Module -**This module supports goal management in the tool.
- **Policy Management Module-** This module supports policy management in the tool.
- **Flesch Readability Index Module-** This module supports requirements that calculate the Flesch Readability Index of policy documents.
- **Scenario Specification and Management Module -** This module supports scenario management in the tool.
- **Requirements Specification Module**- This module supports the requirements for a system.
- **Legal Compliance**
- **Requirements-level Access Control Analysis Framework (RACAF) module-** This section defines the functional requirements that support RACAF.

3. Module Requirements

This section outlines the services to be provided by the tool. Each functional requirement includes: the purpose of the requirement, a brief description, the origin of the requirement and the priority of the requirement. These priorities have been set based on discussions with the stakeholders. SPRAT is a tool bench and will support several other tools. The software will be designed keeping all the layers in mind. But this summer the focus is on implementing the database and high and medium priority requirements for SPRAT and also implement RACAF.

	Priority Level	**Priority Description**
1	High	High priority requirements are critical and must be satisfied. The system may fail if the respective high priority requirements are not satisfied. Additionally, security related requirements are categorized as high priority.
2	Medium	Medium priority requirements are important and desirable, but will not cause the system to fail if not satisfied. These requirements are needed by Qingfeng He for the development of RACAF.
3	Low	Low priority requirements are desirable but not necessary. These requirements are non-critical and can be postponed for implementation in later versions of the system.

3.1. UAM: User Access Module

This section defines the three access levels, specifically outlining permissions and restrictions.

3.1.1. Functional Requirements

FR-UA 1

Requirement Definition: The system shall support an *administrator* level.

Requirement Specification: The *administrator* will have the following privileges:

a. Ability to create user groups such as NCSU TPP.org, GT TPP.org
b. Ability to create project managers, analysts and guests
c. Ability to reset user passwords when needed
d. Ability to disable access for old project managers, analysts and guests. Removing old users implies removing their ability to access the system while still preserving the information entered by them.

Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 1

FR-UA 2

Requirement Definition: The system shall support a *project manager* level.

Requirement Specification: The *project manager* will have the following privileges:

a. Ability to insert a new privacy policy to the repository
b. Ability to delete a privacy policy from the repository
c. Ability to create/add a new domain of privacy policies (e.g, Healthcare, financial, e-commerce, federal agency, etc.)
d. Ability to assign analysts to user groups created by the administrator
e. Ability to assign usergroups and individual analysts to projects
f. Project manager sets restrictions on access to certain kinds of information for guests
g. Ability to export data from a project to an XML file so multiple project managers can use that data
h. Ability to save the current version of the repository so that we can do evolution analysis

Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 1

FR-UA 3

Requirement Definition: The system shall support an *analyst* level.

Requirement Specification: An *analyst* will have the following privileges:

a. Ability to select a privacy policy that has been assigned to them by the project manager.
b. Ability to add, delete and update goals
c. Ability to add, delete and update scenarios
d. Ability to view the details of any goal or a scenario in the repository such as ID, description, source, keyword, taxonomy, actor, occurrence, relevant policy etc.
e. Ability to update personal profile such as name, ID, contact information, usergroups and passwords
f. Ability to add, delete and update requirements
g. Ability to add, delete and update access control policies such as subject, object, action.
h. Ability to view access control policies
i.

Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 1

FR-UA 4

Requirement Definition: The system shall support a *guest* level.

Requirement Specification: The guest will have the following privileges:

a. Ability to view kinds of information in the repository with restrictions set by the project manager. For instance, if a guest is given access permission to a certain privacy policy, he/she will not be able to view goa and scenario ocurrences related to other privacy policies in the repository.

Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 1

3.1.2. Non-Functional Requirements

This section outlines the standards to be followed to ensure that data safety is maintained.

NFR-UAM 1

Requirement Definition: The system shall allow all users to have different access levels to the projects.

Requirement Specification: Each user will have different projects to work on as well as different access levels that will allow them certain privileges within the project.

Origin: Customer Interview (Qingfeng He) 02/06/04

Priority: 1

NFR-UAM 2

Requirement Definition: The system shall allow secure storage of passwords in the database.

Requirement Specification: The system will provide secure storage of passwords of all users in the database.

Origin: Customer Interview (Qingfeng He) 03/02/04

Priority: 1

NFR-UAM 3

Requirement Definition: The system shall allow users to securely log onto the system.

Requirement Specification: The system will provide secure way for users to log onto the system.

Origin: Customer Interview (Qingfeng He) 03/02/04

Priority: 1

3.2. GSM: Goal Specification and Management Module

This section defines the features provided by the tool for goal specification and management

3.2.1. Functional Requirements

FR-GSM 1

Requirement Definition: The system shall allow analysts to add a new goal.

Requirement Specification: The system will allow analysts to enter a new goal into the system as new goals are identified. Following are the necessary elements for each goal:

a. Goal ID
b. Goal Description (not long)
c. Taxonomy Classification
   1. Protection
      - ✓ Notice/Awareness
      - ✓ Choice/Consent
      - ✓ Security/Integrity
      - ✓ Access/Participation
      - ✓ Enforcement/Redress
   2. Vulnerability
      - ✓ Information Monitoring
      - ✓ Information Aggregation
      - ✓ Information Storage
      - ✓ Information Transfer
      - ✓ Information Collection
      - ✓ Information Personalization
      - ✓ Contact
d. Subject Classification
   - ✓ Business Aggregation
   - ✓ Browsing Pattern/Site Usage
   - ✓ CC Information
   - ✓ Children
   - ✓ Customer Information (CI)
   - ✓ Contacting Customer
   - ✓ Contact Institutions
   - ✓ Cookies/Web bugs
   - ✓ Customer System Information
   - ✓ Customer Aggregation
   - ✓ General Information
   - ✓ General User Preference
   - ✓ Identity Theft/Fraud
   - ✓ Law (HIPAA, COPPA, GLBA)
   - ✓ Liability/Responsibility
   - ✓ OPT in /out preferences
   - ✓ Personal Financial Information (PFI)
   - ✓ Personal Health Information (PHI)
   - ✓ Personally Identifiable Information (PII)
   - ✓ PFI/PHI/PII Usage
   - ✓ Policies/Procedures
   - ✓ PP/ToU
   - ✓ Security Access
e. Goal Actor
f. Policy in which the goal was found
g. Granularity Classification (Policy or Scenario goal)
h. Observable/Unobservable
i. Occurrences

j. Context Information (for the goal)
k. Relevant Legislation (e.g, HIPAA, COPPA, GLBA)

Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 3

FR-GSM 2

Requirement Definition: The system shall provide templates for goals, scenarios, P3P statments, EPAL rules and access control policies.

Requirement Specification: These templates will allow analysts to enter detailed information about each goal, scenario, P3P statement, EPAL rule and access control policy that they enter into the tool.

Assumption: Guests are only allowed to view templates.

Origin: Customer interview (Dr. Annie I. Antón) 02/13/04

Priority: 3

FR-GSM 3

Requirement Definition: The system shall allow analysts to classify goals.

Requirement Specification: The system will allow the administrator, project manager and analysts to classify goals in the following categories:

a. *Policy goals* or *scenario goals*
b. *Observable goals* or *unobservable goals*
c. P*rotection goals* or *vulnerabilities*
d. Goals based on *subject classification*

Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 3

FR-GSM 4

Requirement Definition: The system shall allow multiple subject classifications for each goal.

Requirement Specification: The system will allow analysts to choose multiple subject classifications for each goal. For instance, a goal could be a part of ‘security access’ as well as ‘personal health information.’

Origin: Customer interview (Qingfeng He) 03/02/04

Priority: 3

FR-GSM 5

Requirement Definition: The system shall provide the ability to dynamically add a new classification type of goals to the tool.

Requirement Specification: The system will allow the project manager to add a new classification type of goals.

Origin: Customer interview (Qingfeng He) 03/02/04

Priority: 3

FR-GSM 6

Requirement Definition: The system shall allow the analysts to request a new classification type of goals and also allow the project manager to create that classification type.

Requirement Specification: The system shall allow the analysts to request a new classification type of goals and also allow the project manager to create that classification type.

Origin: Customer interview (Dr. Annie I. Antón) 07/12/04

Priority: 3

FR-GSM 7

Requirement Definition: The system shall provide the ability to update an existing goal.

Requirement Specification: The system will analysts to edit an existing goal in the system.

Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 3

FR-GSM 8

Requirement Definition: The system shall provide the ability to delete a goal.

Requirement Specification: The system will analysts to delete an existing goal from the repository.

Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 3

FR-GSM 9

Requirement Definition: The system shall provide the ability to automatically propagate associated policy information upon deletion or replacement of a goal.

Requirement Specification: The system will provide a way to merge goals into policies to reduce time spent on the goal reconciliation process. For instance, if goal A is deleted from the repository and replaced by a new goal B, all the policies where goal A appeared should be updated automatically to include goal B.

Origin: Customer interview (Dr. Annie I. Antón) 02/13/04

Priority: 3

FR-GSM 10

Requirement Definition: The system shall maintain traceability links between a goal and the policy from which the goal was derived.

Requirement Specification: The system will allow analysts and guest to choose a goal and then the system will display all the policies in which that particular goal appears.

Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 3

FR-GSM 11

Requirement Definition: The system shall provide the ability to display the number of occurrences of a goal in a policy, in multiple policies and within a domain.

Requirement Specification: The system will allow analysts and guest to choose a policy and a goal and then the system will allow analysts and guests to view the total occurrences of that particular goal in the chosen policy.

Note: For ACP, it is important to know who the system will display this information to.
Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 3

FR-GSM 12

Requirement Definition: The system shall provide the ability to display the number of different goals that occur in a policy.

Requirement Specification: The system will allow analysts and guests to choose a policy and then the system will allow analysts and guests to view the the number of different goals that occur in that policy. For instance, if the user chooses a health policy and there were 4 different goals found in that policy then the system will display 4. However, the policy might have those 4 goals repeated a number of times.

Origin: Customer interview (Qingfeng He) 03/02/04

Priority: 3

FR-GSM 13

Requirement Definition: The system shall display the context of a goal.

Requirement Specification: The system will allow analysts and guests to choose a goal and the system will then allow analysts and guests to view the context of the goal, which is the actual statement from the policy in which the goal originally appeared.

Origin: Customer interview (Neha Jain) 03/03/04

Priority: 3

FR-GSM 14

Requirement Definition: The system shall allow analysts to create and update goal *keyword definitions* and allow guests to view keyword definitions.

Requirement Specification: The system will provide a way to display the definition of the goal keywords in the SPRAT for convenient access. For instance, the keyword 'ALLOW' will have its definition associated with it. Additionally, the system will provide the ability to access these definitions in a separate section.

Origin: Customer interview (Dr. Annie I. Antón) 02/06/04

Priority: 3

FR-GSM 15

Requirement Definition: The system shall provide the ability to lock and unlock the keyword definition by either the project manager or the first person who created the definition in the repository.

Requirement Specification: The system shall provide the ability to lock and unlock the keyword definition by either the project manager or the first person who created the definition in the repository.

Origin: Customer interview (Dr. Annie I. Antón) 07/13/04

Priority: 3

FR-GSM 16

Requirement Definition: The system shall allow analysts and guests to search goals according to analyst chosen attributes.

Requirement Specification: The system will generate a list of all goals that have the same source, actor, subject etc. upon analyst's request. This will allow the analyst to determine effects caused by a change in conditions or can provide quick feedback on what goals need further elaboration.

Origin: Customer interview (Neha Jain) 03/03/04

Priority: 3

FR-GSM 17

Requirement Definition: The system shall allow analysts to view elements of a goal returned by a query.

Requirement Specification: The system will provide analysts the ability to view full details of any goal returned by a query.

Origin: Customer interview (Neha Jain) 03/03/04

Priority: 3

FR-GSM 18

Requirement Definition: The system shall provide a template to express goals in BNF grammar.

Requirement Specification: This template will conform to the BNF grammar of allowable structure. E.g.,
<Goal> ::= <keyword> <subject> <action>;

Origin: Customer interview (Qingfeng He) 02/13/04

Priority: 3

FR-GSM 19

Requirement Definition: The system shall support conflict identification and resolution.

Requirement Specification: The system will provide a mechanism to automate the identification of conflicts between requirements and privacy policies.

Origin: Customer interview (William Stufflebeam) 03/30/04
This was a suggestion from his review of Annie's paper. Definitely needs elaboration

Priority: 3

FR- GSM 20

Requirement Definition: The system shall allow analysts to view scenarios associated with individual scenarios.

Requirement Specification: When the analyst views the full details of a scenario, the system will indicate the goals that are shared among scenarios.

Origin: Customer interview (Dr. Annie I. Antón) 06/25/04

Priority: 3

FR- GSM 21

Requirement Definition: The system shall provide a P3P dedicated section in the tool.

Requirement Specification: The elements of the section will include: specification, rationale, a drop down box with options such as yes, no or partial.

Origin: Customer interview (Dr. Annie I. Antón) 06/25/04

Priority: 3

FR- GSM 22

Requirement Definition: The system shall provide an EPAL dedicated section in the tool.

Requirement Specification: The elements of the section will include: specification, rationale, a drop down box with options such as yes, no or partial.

Origin: Customer interview (Dr. Annie I. Antón) 06/25/04

Priority: 3

3.3. ADM: Analysis Document Management Module

There are different kinds of analysis documents, such as policy documents. This section defines the features for the document management module.

3.3.1. Functional Requirements

FR-ADM 1

Requirement Definition: The system shall allow project managers to add analysis documents and assign a domain to each document.

Requirement Specification: The system will allow the project manager to add policies documents repository and assign a domain to each document. The domain could be healthcare, financial or e-commerce.

Origin: Customer interview (Qingfeng He) 02/06/04
This will require simply adding the policy to the tool and not going through and manually changing the code to add the policy. This is implementation bias but is something Qingfeng wanted to add here.

Priority: 3

FR-ADM 2

Requirement Definition: The system shall allow project managers to edit the domain for the documents.

Requirement Specification: The system will allow the project manager to edit the domain for the documents such as change the domain name.

Origin: Customer interview (Dr. Annie I. Antón) 07/13/04

Priority: 3

FR-ADM 3

Requirement Definition: The system shall allow project managers to delete the domain for the documents.

Requirement Specification: The system will allow the project manager to delete the domain for the documents.

Reasoning: We make errors

Origin: Customer interview (Dr. Annie I. Antón) 07/13/04

Priority: 3

FR-ADM 4

Requirement Definition: The system shall allow project managers to create document types.

Requirement Specification: The system will allow the project manager to create document type such as policy documents, requirements document, manuals etc.

Origin: Customer interview (Dr. Annie I. Antón) 07/12/04

Priority: 3

FR-ADM 5

Requirement Definition: The system shall provide the ability to display document names and links to the actual document text within a specific domain in an alphabetical order.

Requirement Specification: The system will allow analysts and guest to view policies in the system in an alphabetical order.

Origin: Customer interview (Neha Jain) 02/06/04

Priority: 3

FR-ADM 6

Requirement Definition: The system shall allow project managers to create a new domain and assign existing documents to this domain.

Requirement Specification: The system will allow project managers to create a new domain for the documents and assign existing documents to that particular domain.

Origin: Customer interview (Dr. Annie I. Antón) 06/25/04

Priority: 3

FR-ADM 7

Requirement Definition: The system shall support automatic multi-user analysis results comparison upon the project manager's request.

Requirement Specification: The system will allow analysts to classify goals separately and as a result they can automatically check the difference in their classification results for their resolution.

Constraint: Other analyst's classification must be withheld by the system until the given analyst has completed his/her classification. At that time the analyst will be able to view the other analyst's classifications. This is to prevent bias.

Note: Need to check with Dr. Earp what statistical analysis must be carried out behind the scenes and add that as a new requirement.

Origin: Customer interview (Qingfeng He) 02/06/04

Priority: 3

3.4. FRE: Flesch Readability Module

This section contains requirements that calculate the Flesch Readability Index of policy documents.

3.4.1. Functional Requirements

FR-FRE 1

Requirement Definition: The system shall provide a way calculate the *Flesch Readability for textual documents.*

Requirement Specification: The system will provide analysts way to calculate the Flesch Readability Score (FRES) and Flesch-Kincaid Grade Level (FGL) for textual documents. For this, a link to the actual textual document as well as the corresponding FRES and FGL as the number of words and sentences in each document will be provided.

Origin: Customer interview (Dr. Annie I. Antón) /03/26/04

Priority: 2

3.5. SSM: Scenario Specification and Management

This section defines the features associated with scenarios specification and management.

3.5.1. Functional Requirements

FR- SSM 1

Requirement Definition: The system shall provide the ability to add a scenario to the system.

Requirement Specification: The system shall allow analysts to add a scenario to the system. Following are the necessary elements for each scenario:

- Scenario Name
- Sources
- Actor(s)
- Event(s)
- Action(s)
- Obstacle(s)
- Constraint(s)
- Pre-Condition(s)
- Post-Condition(s)
- Status
- Issue(s)- *These are questions that come up: catch on*
- Goals
- Requirements

Origin: Customer interview (William Stufflebeam) 03/02/04

Priority: 1

FR- SSM 2

Requirement Definition: The system shall allow analysts to edit/modify a scenario within a project

Requirement Specification: The system shall allow analysts to edit/modify a scenario within a project.

Origin: Customer interview (William Stufflebeam) 03/02/04

Priority: 3

FR- SSM 3

Requirement Definition: The system shall provide the ability to delete a scenario from a project without deleting it from the system

Requirement Specification: The system shall allow analysts to delete a scenario from the system.

Origin: Customer interview (William Stufflebeam) 03/02/04

Priority: 1

FR- SSM 4

Requirement Definition: The system shall allow analysts to reuse other scenarios.

Requirement Specification: The system shall allow analysts to reuse other scenarios when specifying a scenario.

Origin: Customer interview (William Stufflebeam) 03/02/04

Priority: 1

FR- SSM 5

Requirement Definition: The system shall allow analysts to view goals associated with individual scenarios.

Requirement Specification: When the analyst views the full details of a goal, the system will indicate the scenarios that are shared among goals.

Origin: Customer interview (William Stufflebeam) 03/02/04

Priority: 3

FR- SSM 6

Requirement Definition: The system shall allow analysts to view the elements of any scenario in the project.

Requirement Specification: The system shall allow analysts to view the elements of any scenario in the project assigned to this analyst.

Origin: Customer interview (William Stufflebeam) 03/02/04

Priority: 1

FR-SSM 7

Requirement Definition: The system shall generate a list of all scenarios that share the same attribute or sets of attributes

Requirement Specification: The system will allow analysts to generate list of all scenarios that have the same source, goal, actor, etc. This will allow the analyst to determine effects caused by a change in conditions or can provide quick feedback on what scenarios need further elaboration.

Origin: Customer interview (Neha Jain) 03/03/04

Priority: 2

3.6. RS: Requirements Specification Module

This section defines the requirements specifications.

3.6.1. Functional Requirements

FR-RS 1

Requirement Definition: The system shall provide the ability to specify requirements.

Requirement Specification: The system will allow analysts to specify requirements.

Origin: Customer interview (Neha Jain) 04/07/04

Priority: 3

FR-RS 2

Requirement Definition: The system shall provide the ability to add a requirement.

Requirement Specification: The system will allow analysts to add requirements to the system. The requirement will include the following:

-Goals
-Constraints

Origin: Customer interview (Neha Jain) 07/09/04

Priority: 3

FR-RS 3

Requirement Definition: The system shall provide the ability to delete a requirement.

Requirement Specification: The system will allow analysts to delete requirements from the system.

Origin: Customer interview (Neha Jain) 07/09/04

Priority: 3

FR-RS 4

Requirement Definition: The system shall provide the ability to edit a requirement.

Requirement Specification: The system will allow analysts to edit requirements.

Origin: Customer interview (Neha Jain) 07/09/04

Priority: 3

FR-RS 5

Requirement Definition: The system shall provide a template for specifying requirements.

Requirement Specification: The system will provide a template to specify requirements.

Origin: Customer interview (Neha Jain) 07/09/04

Priority: 3

3.7. LC: Legal Compliance Module

This section defines the legal compliance for privacy policies.

3.7.1. Functional Requirements

FR-LC 1

Requirement Definition: The system shall provide a demo version of the tool

Requirement Specification: The system will provide a trial version of the tool allowing people to enter about 30 objects and try our system.

Origin: Customer interview (William Stufflebeam) 07139/04

Priority: 3

3.8. RACAF: Requirements-level Access Control Analysis Framework Module

This section defines the functional requirements that support RACAF.

I. Data Analysis

FR-RACAF 1

Requirement Definition: The system shall allow analysts to add new objects (names, types and other attributes).

Requirement Specification: The system shall allow analysts to add new objects. Elements of an object include: name, type, hierarchical information, preferences, etc.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 1

FR-RACAF 2

Requirement Definition: The system shall support association of privacy preferences with objects.

Requirement Specification: The system shall allow analysts to associate privacy preferences with objects. Elements of a privacy preference include: purpose, recipient, retention, consent, etc.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 1

FR-RACAF 3

Requirement Definition: The system shall support hierarchical structure of dataand its type.

Requirement Specification: The system shall allow analysts to specify hierarchies to organize data and its types.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 1

FR-RACAF 4

Requirement Definition: The system shall allow graphical view of data structures.

Requirement Specification: The system shall allow analysts to view data hierarchies graphically.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 3

II. Task Analysis

FR-RACAF 5

Requirement Definition: The system shall support deriving access control elements.

Requirement Specification: The system shall allow analysts to specify access control elements.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 1

FR-RACAF 6

Requirement Definition: The system shall allow analysts to view scenario elements and edit access control rules at the same time.

Requirement Specification: The system shall allow analysts to view scenario elements on the left hand of the screen and edit access control rules on the right hand of the screen.

Origin: Customer interview (Dr. Annie I. Antón) 06/25/04

Priority: 1

III. Organizational Structure Analysis

FR-RACAF 7

Requirement Definition: The system shall support a hierarchical representation of organizational structures.

Requirement Specification: The system shall allow analysts to specify business and organizational structures.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 1

FR-RACAF 8

Requirement Definition: The system shall support the representation of organizational boundaries.

Requirement Specification: The system shall allow analysts to specify organization boundaries via the use of roles.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 1

FR-RACAF 9

Requirement Definition: The system shall support the representation of actor relationships.

Requirement Specification: The system shall allow analysts to specify relationships among actors.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 1

FR-RACAF 10

Requirement Definition: The system shall support the definition of roles.

Requirement Specification: The system shall allow analysts to specify roles.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 1

FR-RACAF 11

Requirement Definition: The system shall support role delegation.

Requirement Specification: The system shall allow project managers to delegate their responsibilities to analysts for a specific time frame.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 1

IV. Information Analysis

FR-RACAF 12

Requirement Definition: The system shall support analysis of a specific type of data flow within or across the boundary of an organization, given a set of access control policies.

Requirement Specification: The system shall allow analysts to graphically view the allowable flows for specific types within an organization and across multiple organizations given a set of access control policies.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 3

V. Access Control Policy Specifications

FR-RACAF 13

Requirement Definition: The system shall support access control specification using Ponder language.

Requirement Specification: The system shall allow analysts to invoke the ponder policy editor.

Reasoning: Because Ponder provides tool support for policy specification, SPRAT shall provide interface support to interact with Ponder editor.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 1

VI. Formal Verification

FR-RACAF 14

Requirement Definition: The system shall provide partial support for translating Ponder policy into Alloy specifications for security verification.

Requirement Specification: The system shall provide partial support for translating Ponder policy into Alloy specifications for security verification. “Partial support” means providing as much automatic translation as possible so that manual specification of Alloy could be minimized. The partial support also includes providing interface between Ponder editor and Alloy tool.

Origin: Customer interview (Qingfeng He) 05/14/04

Priority: 3

3.9. P3P: P3P Module

FR-P3P 1

Requirement Definition: The system shall provide a way to extract goals data-usage information from a *P3P privacy policy* according to the P3P standard.

Requirement Specification: The system will provide users a way to extract goalsinformation which is the information pertaining to the usage of a data-item from a P3P privacy policy according to the P3P standard. This involves parsing the respective P3P documents- privacy policy documents or the user’s privacy preferences.

Origin: Customer interview (Bharathy) /03/25/04

Priority: 3

FR-P3P 2

Requirement Definition: The system shall provide a way to extract goalsdata-usage information according toas per the user’s privacy preferences in accordance with the P3P standard.

Requirement Specification: The system will provide users a way to extract goals which is the information pertaining to the usage of a data-item accordings per to the user’s privacy preferences in accordance with the P3P standard. Here the goalsinformation pertaining necessary to accepting as well as rejecting a policy according to user’s privacy preferences are extracted. This involves obtainingparsing the respective documents- privacy policy documents or the user’s privacy preferences and deriving the goalspertinent rules from them.

Origin: Customer interview (Bharathy) /03/25/04

Priority: 3

FR-P3P 3

Requirement Definition: The system shall provide a way to capture the mined goalsinformation from the P3P policy into a database corresponding to a P3P privacy policy.

Requirement Specification: The system will provide users a way to concisely capture goalsinformation mined from the P3P policy, into a database corresponding to a P3P privacy policy.

Origin: Customer interview (Bharathy) /03/25/04

Priority: 3

FR-P3P 4

Requirement Definition: The system shall provide a way to capture the mined goalsinformation from the user's privacy preferences into a database corresponding to the user's privacy preferences.

Requirement Specification: The system will provide users a way to concisely capture goalsthe rules derived from the user's privacy preferences into a database corresponding to the user's privacy preferences.

Origin: Customer interview (Bharathy) /03/25/04

Priority: 3

FR-P3P 5

Requirement Definition: The system shall provide a way to evaluate the information extracted from the P3P privacy policy against the information extracted from the user's privacy preferences.

Requirement Specification: The system will provide users an unambiguous way to evaluate the information extracted from the privacy policy against the information extracted from the user's privacy preferences. During the evaluation, following scenarios need to be dealt with:

If the data-usage goals information mined from the P3P policy match those from the user's privacy preferences corresponding to both acceptance and rejection of a policy, then a conflict should be detected and a notification requiring user's intervention raised.

If the goals data-usage information mined from the P3P policy match those from the user's privacy preferences corresponding to either accepting or rejecting a policy, the policy should be accepted or rejected respectively.

If the goals data-usage information mined from the P3P policy does not match those from the user's privacy preferences corresponding to either acceptance or and rejection of a policy, then again a conflict should be detected and a notification requiring user's intervention raised.

Origin: Customer interview (Bharathy) /03/25/04

Priority: 3

4. System Requirements

This section outlines *constraints* on the system in order to provide for compatibility, security and privacy as defined by the customer.

SR 1

Requirement Definition: The system shall generate an access log for every add, delete and edit action in the system.

Requirement Specification: The system will generate an access log for every add, delete and edit action in the system for the purpose of future tracking. General elements of an access log contain time, date, user id, action and object..

Rationale: When multiple users are working on the tool at the same time

Origin: Customer Interview (William Stufflebeam) 03/02/04

Priority: 1 (since it is needed for empirical study)

5. Requirements Traceability Matrix

This section outlines requirement dependencies.

6. Document Revision History

This section outlines the version of the current document being used, the people responsible for the document, dates the document is modified and the changes made to the document.

Version	1.0.0
Name(s)	Neha Jain
Date of last change	02/13/2004
Change Description	First document version created

Version	1.0.1
Name(s)	Neha Jain
Date of last change	02/23/2004
Change Description	Refined requirements after talking to customer. New

	requirements were added namely, GM 7, GM 8, GM 9, GM 10. Some requirements were deleted namely, PM 6, BS 1

Version	1.0.2
Name(s)	Neha Jain
Date of last change	03/02/2004
Change Description	Further refined requirements after talking to customer. UAL 2 and 4 were merged and UAL 1 and 3 were redefined. The Goal Management module was completely restructured. PM 1 and PM 4 were deleted. Three new modules were added namely, Scenario management, requirements specification and legislations.

Version	1.0.3
Name(s)	Neha Jain
Date of last change	03/05/2004
Change Description	Further refined requirements after talking to customer. Added GSM 4, GSM 5, GSM 14, SPR 4, SPR 5, SSC 1. Added glossary terms, scenario specification and management module Removed Browser support section, removed SPR 3.

Version	1.0.4
Name(s)	Neha Jain
Date of last change	03/19/2004
Change Description	Further refined requirements after talking to customer. Added GSM 16. Refined glossary terms. Deleted SSC1.

Version	1.0.5
Name(s)	Neha Jain
Date of last change	03/26/2004
Change Description	Refined glossary and content of introduction.

Version	1.0.6
Name(s)	Neha Jain
Date of last change	04/09/2004
Change Description	Added PM5, 6, 7, 8, 9

Version	1.0.7

Name(s)	Neha Jain
Date of last change	05/05/2004
Change Description	Grammar corrections, enhanced glossary items

Version	1.0.8
Name(s)	Neha Jain
Date of last change	05/14/2004
Change Description	Consistency check, rearranged requirements to ensure they were in the correct module. Set priorities for requirements.

Version	1.0.9
Name(s)	Neha Jain
Date of last change	05/19/2004
Change Description	Added RACAF requirements.

Version	2.00
Name(s)	Neha Jain
Date of last change	07/12/2004
Change Description	Added Annie’s and Qingfeng’s changes and new requirements.

7. Appendix

Glossary

This section contains glossary of the terms used throughout the document.

Administrator: A super user who has the ability to grant/deny access to anyone he/she chooses.

Analyst: A user who is a member of the project team and analyzes the policies assigned to him/her.

Constraint: A constraint is a limit to a system entity. It restricts possible occurrences or allowable combinations in relationship sets, interactions, object sets, etc.

Customer: The customer is the originator of requirements, and hence, external to the organization that actually provides the support. Whether the customers are internal or external to your organization, they use the product provided by the software developers as an input to their work processes. Almost anyone you interact with is a customer.

Database*:* An electronic collection of data stored in an organized and searchable manner.

Goal: A goal is an objective of the system under consideration.

Goal Actor: An agent responsible for achieving the associated goal.

Goal Reconciliation: The process of comparing goals to identify conflicts, redundancies and synonymous goals and resolve discrepancies.

Goal Mining: The process of reading privacy policies and extracting goals from them.

Goal Management: The process of organizing the goals collected from the policies in a readable and easy to access form.

Project Manager: A user who has access to all elements of a project and delegates work to other members.

Privacy Policy: A privacy policy is a web site's official statement on: 1. what personal information is being collected. 2. how the information is being used. 3. how an individual can access their own data. 4. how an individual can opt-out. 5. what security measures are in place to protect the user's information during the collection process and in storage [1]

Privacy Goals and Scenario Goals:
A ***Policy goal*** reflects general high-level enterprise policies, whereas a ***scenario goal*** envisions possible usage situations or practices. Scenario goals are usually instantiations of policy goals, thus having the advantages of being concrete, easier for user to understand and the disadvantage of not

being exhaustive. This classification is similar to the distinction between strategic goals and tactical goals in requirements engineering [2] and [3].

Priority level: This prioritizes the requirements in low, medium or high level.

Project: A project is a document or multiple documents, which need to be analyzed. These documents can be privacy policies of companies, terms and conditions, handbooks, manuals etc.

Security: The security of a system is the extent of protection against some unwanted occurrence such as the invasion of privacy, theft, and the corruption of information or physical damage.

Observable (visible) and Unobservable (invisible) Goals:

Observable privacy goals are those that are extracted in such a way that an average Internet user is aware of data collection while assessing websites with a browser using default security and privacy settings. This is a conscious process and easy to conclude. Information is voluntarily given, shared and used. For instance, emails, surveys, forms.

Unobservable privacy goals are those that are extracted in a hidden manner that requires users to take a proactive role in learning about website privacy practices (e.g, reading a privacy policy, setting the browser's security and privacy settings, learning about cookie, etc.). This is a subconscious process and difficult for consumers to conclude. Information is voluntarily given, shared and used.

Traceability: The ability to trace the history, application or location of an item or activity by means of recorded identification.

Context: Text surrounding a passage under examination that may throw light on the goals extracted.

Subject Classification

- ✓ Unclassified
- ✓ Business Aggregation
- ✓ Browsing Pattern/Site Usage
- ✓ CC Information
- ✓ Children
- ✓ Customer Information (CI)
- ✓ Contacting Customer
- ✓ Contact Institutions
- ✓ Cookies/Web bugs
- ✓ Customer System Information
- ✓ Customer Aggregation
- ✓ General Information
- ✓ General User Preference
- ✓ Identity Theft/Fraud
- ✓ Law(HIPAA, COPPA, GLBA)
- ✓ Liability/Responsibility
- ✓ OPT in /out preferences
- ✓ Personal Financial Information (PFI)
- ✓ Personal Health Information (PHI)

- ✓ Personally Identifiable Information (PII)
- ✓ PFI/PHI/PII Usage
- ✓ Policies/Procedures
- ✓ PP/ToU
- ✓ Security Access

Keyword definitions
P3P privacy policy
Felsch Readability Index

Acknowledgement

We would like to thank the National Science Foundation (NSF) for supporting our research efforts.

References

This section contains references used in this document.

1. www.ecommerce-dictionary.com/p.html

2. [AHB04] Annie I. Antón, Qingfeng He, and Davide Bolchini. The Use of Goals to Extract Privacy and Security Requirements from Policy Statements. Submitted to: The 12th International Requirements Engineering Conference (RE'04), January 26, 2004.

3. [AEB04] Annie I. Antón, Julia B. Earp, Davide Bolchini, Qingfeng He, Carlos Jensen and William Stufflebeam. The Lack of Clarity in Financial Privacy Policies and the Need for Standardization, Accepted, to appear in: IEEE Security & Privacy, 2004.

4. [JEA02] Olli Jarvinen, Julia B. Earp and Annie I. Antón. A Visibility Framework for Privacy Management Requirements. *2nd Symposium on Requirements Engineering for Information Security*, Raleigh, NC, 15 October 2002.