

Strategies for Developing Policies & Requirements for Secure e-Commerce Systems

Annie I. Antón
College of Engineering
(aianton@eos.ncsu.edu)

Julie B. Earp
College of Management
(julia_earp@ncsu.edu)

NC STATE UNIVERSITY



Agenda

- Background of the problem
- Addressing the problem
- Strategies
- Work in progress
- Future work



The Problem

E-Commerce systems fail to adequately address security and privacy issues during analysis & design.

The Problem

- ❑ Generating security requirements
- ❑ Defining privacy protections
- ❑ Need for prescriptive guidance to develop policy requirements *[Trcek, PFIRES]*
 - Security policy
 - Privacy policy

Addressing the Problem

❑ Goal

- establish effective approaches for security and privacy *requirements coverage*

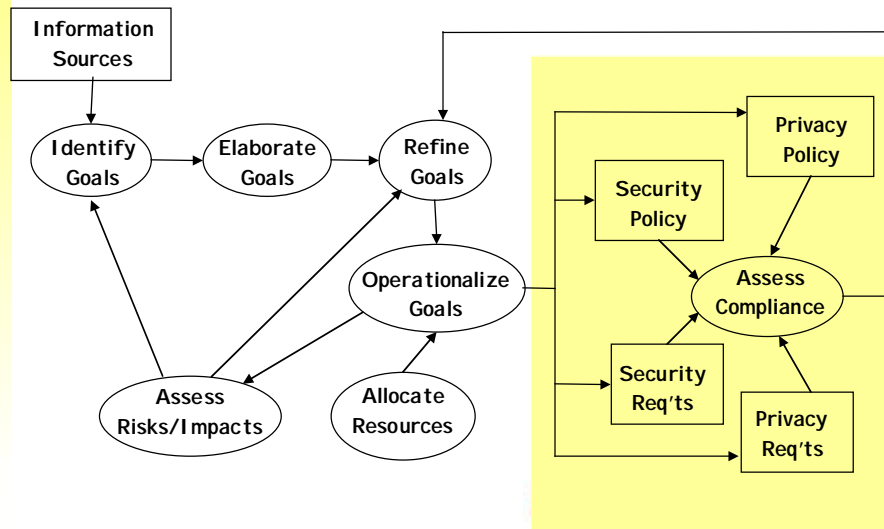
❑ Strategy

- apply scenario management and goal-driven analysis strategies
- perform risk and impact assessments to ensure system requirements align with organizational policies
- analyze security and privacy policies
- provide tool support w/ reusable library of goals for EC
- validate methods with real-world industry EC systems

Goal-Driven RE

- ❑ Requirements must be stated accurately before they can be implemented correctly
- ❑ Obtaining requirements is conceptually complex
- ❑ Enterprise goals are more stable than system requirements
- ❑ Transforming enterprise and systems goals into requirements is ill-defined and prone to information loss
...
- ❑ Goals have become an active area of work in RE
- ❑ Focus on the DISCOVERY of requirements

Using the GBRAM for Policy Formulation & RE



Goal Classes and Security Policies

GBRAM Goal Classes	Common Security Policies
User Goals	User behavior
System Goals	Access to data Administration
Communication Goals	Administration
Security Goals	Password Remote access Extranet/Internet Incident response
Knowledge Goals	User identification Access to data Security monitoring & audit
Quality Goals	Security monitoring & audit

Goals, Obstacles & Scenarios

- | | |
|--|---|
| <ul style="list-style-type: none"> ❑ <i>Goal:</i> <ul style="list-style-type: none"> – RELEASE info only with permission from customer ❑ <i>Obstacle:</i> <ul style="list-style-type: none"> – Customer might not know about options available ❑ <i>Scenario:</i> <ul style="list-style-type: none"> – Customer selects PII usage preferences | <ul style="list-style-type: none"> ❑ <i>Goal:</i> <ul style="list-style-type: none"> – PROVIDE access to customer's PII ❑ <i>Obstacle:</i> <ul style="list-style-type: none"> – PII server down – Server doesn't recognize customer ❑ <i>Scenarios:</i> <ul style="list-style-type: none"> – Update PII – Correct inaccuracies |
|--|---|

Compliance: Policy Statements & Requirements

	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.			X
The firewall should be configured to limit data access to authorized member users.	✓	✓	



Current work

- ❑ *Goal mining* for security requirements
 - extracting pre-requirements goals from post-requirements text artifacts
- ❑ Taxonomy:
 - Privacy Protection Goals
 - Optative & Indicative Goals
 - Respective Requirements
- ❑ Library of stable, reusable privacy and security goals for SMART

Privacy Policy Analysis

- ❑ ISPs
 - AOL
 - Earthlink
 - Free Internet
- ❑ Online Retailers
 - Amazon
 - eNews
 - ToySmart
- ❑ Traditional M.O. Catalog
 - Banana Republic
 - Eddie Bauer
 - JCrew
- ❑ Auction Sites
 - Ebay
 - Reverse Auction
 - Sothebys
- ❑ Drug Stores
 - Drugstore.com
 - Eckerd Drugs
 - Long Drugs
- ❑ Grocery Stores
 - HomeGrocer
 - Lowes
 - Peapod
- ❑ Travel Agencies
 - American Express
 - Expedia
 - Travelocity
- ❑ Trust Services
 - BBBOnline
 - TRUSTe
 - Verisign

Preliminary Taxonomy

- ❑ Optative Privacy Goals
 - Access/Participation
 - Choice/Consent
 - Enforcement/Redress
 - Integrity/Security
 - Notice/Awareness
- ❑ Indicative Privacy Goals
 - Aggregation of Information
 - Collection of Information
 - Monitoring of Information
 - Personalization
 - Solicitation
 - Storage of Information
 - Transfer of Information

Summary & Future Work

- ❑ Contribution
 - introduce effective approaches for security and privacy requirements specification & coverage
- ❑ Currently
 - Privacy policies
 - SMaRT under development
- ❑ Next
 - Analyze security policies for goal classes
 - Defining security policy requirements
 - Validation in NCSU e-Commerce Studio

E-Commerce .edu 

SREIS - 1st Symposium on RE for Information Security

- ❑ March 5-6, 2001 -- Indianapolis, Indiana
- ❑ Co-sponsored by:
 - Purdue University CERIAS
 - E-commerce program at NCSU
 - NIST
- ❑ In cooperation w/ ACM SIGSOFT & SIGACT
- ❑ <http://www.cerias.purdue.edu/SREIS.html>



E-Commerce .edu 