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

E-Commerce.edu

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 \cite{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

<table>
<thead>
<tr>
<th>GBRAM Goal Classes</th>
<th>Common Security Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Goals</td>
<td>User behavior</td>
</tr>
<tr>
<td>System Goals</td>
<td>Access to data</td>
</tr>
<tr>
<td></td>
<td>Administration</td>
</tr>
<tr>
<td>Communication Goals</td>
<td>Administration</td>
</tr>
<tr>
<td>Security Goals</td>
<td>Password</td>
</tr>
<tr>
<td></td>
<td>Remote access</td>
</tr>
<tr>
<td></td>
<td>Extranet/Internet</td>
</tr>
<tr>
<td></td>
<td>Incident response</td>
</tr>
<tr>
<td>Knowledge Goals</td>
<td>User identification</td>
</tr>
<tr>
<td></td>
<td>Access to data</td>
</tr>
<tr>
<td></td>
<td>Security monitoring &amp; audit</td>
</tr>
<tr>
<td>Quality Goals</td>
<td>Security monitoring &amp; audit</td>
</tr>
</tbody>
</table>
Goals, Obstacles & Scenarios

- **Goal:** RELEASE info only with permission from customer
- **Obstacle:** Customer might not know about options available
- **Scenario:** Customer selects PII usage preferences

- **Goal:** PROVIDE access to customer's PII
- **Obstacle:** PII server down
- **Scenario:** Update PII

Compliance: Policy Statements & Requirements

<table>
<thead>
<tr>
<th>Authentication is required for access to the commerce Web server.</th>
<th>MAINTAIN member entrance to server</th>
<th>ENSURE content visibility to members only</th>
<th>MAINTAIN member data history (for user customization)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All member account information will be kept confidential and used for internal business purposes only.</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>The firewall should be configured to limit data access to authorized member users.</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
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
  - J.Crew
- 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

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 with ACM SIGSOFT & SIGACT
- http://www.cerias.purdue.edu/SREIS.html