The Evolution of Information Systems Security Design Methods

<table>
<thead>
<tr>
<th>Generation</th>
<th>Primary Features</th>
<th>Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Generation -</td>
<td>Checklist Methods (1972 - 1)</td>
<td>Map of limited solution</td>
</tr>
<tr>
<td></td>
<td></td>
<td>on the information problem</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Survey available elements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>solution that matches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>functional requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>solve each functional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>requirement</td>
</tr>
<tr>
<td>Third Generation -</td>
<td>Logical-Transformational Methods (1988 - 3)</td>
<td>Highly abstracted design</td>
</tr>
<tr>
<td></td>
<td></td>
<td>expressing problem and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>solution space</td>
</tr>
</tbody>
</table>

The Problems in the Area of Information Systems Security Design

1. Information Security is not addressed at the early stages of information systems design in a comprehensive way;
2. Although business experts have knowledge about business-driven and law-driven security needs, they have no ability to express security needs in a clear, non-technical way;
3. There is a communication gap between business and security experts;
4. In inter-organisational business processes the above problems are compounded by the necessity to achieve consistency between security policies and control across several organisations.

The Initially Proposed Scheme of the Design of a Secure Information System

The scheme combines use of SSM, risk analysis and UML case and scenario case diagrams and may be used for development of a new secure IS and for the vulnerabilities analysis of the existing IS and countermeasures planning. Business and security specialists must come to a common design.

The Feedback for the Initial Stage of the Research

- The subject is too broad
- The results are difficult to verify
- A long time needed to implement
- Hard to find a case-study

The need to narrow the area of the research down.

What are the initial stages of the Information System Design? Business Process Modelling

The GAPS in the Existing Research

Based on the analysis conducted, four gaps in the existing research were identified:
1) There is no security extension for the Business Motivation Model (BMM);
2) The existing security extensions for the BPMN are not comprehensive;
3) There is no security extension developed for the choreography diagram in the BPMN 2.0;
4) There is no procedure developed for the translation of security requirements expressed in the BMM into the security annotated BPMN model. All four areas are closely linked together. Nevertheless, it will be impossible to investigate all four topics. Therefore, it was decided to concentrate on the second and third topics.

The Requirements for the New Security Modelling Extension

The analysis of the existing business process modelling notations and of the existing security modelling extensions allowed derivation of the requirements for the new security modelling extension. Thus, the new extension should:
- Be based on the contemporary comprehensive model of Information Security;
- Be graphical and easily understood by business experts with technical security background;
- Be platform-independent and business-oriented;
- Enable business experts to express security concerns or needs at the stage of business process modelling;
- Serve as a bridge between business and security experts;
- Allow consideration of security concerns at the early stage of cross-organisational projects;
- Allow seeing a "big picture" of an overall inter-organisational business process;
- Help to improve level of trust between the organisations involved in information sharing.

The Future Work

- The Short-term Research Agenda
  - Write a critical evaluation of the existing security modelling extensions;
  - Explore the business processes in B&C Projects (e.g. the RIBA plan of work);
  - Develop a set of BPMN diagrams for a generic B&C Project;
  - Examine security concerns, needs and requirements, as well as the current state of InfoSec in the field of B&C;

- The Long-term Research Agenda
  - Develop a concept of a security modelling extension, which will meet the needs of B&C Projects;
  - Develop a software tool, based on the new security modelling concept;
  - Test the new security modelling extension and receive the evaluation from the industrial partners.