A Comprehensive Security Modelling Extension for the BPMN.

The Integration of Security into Business Process Management.

Yulia Cherdantseva, Jeremy Hilton, Omer Rana

{y.v.cherdantseva,omer.f.rana}@cs.cardiff.ac.uk, j.c.hilton@cranfield.ac.uk

How to Design a Secure Information System?

The Evolution of Information Systems Security Design Methods

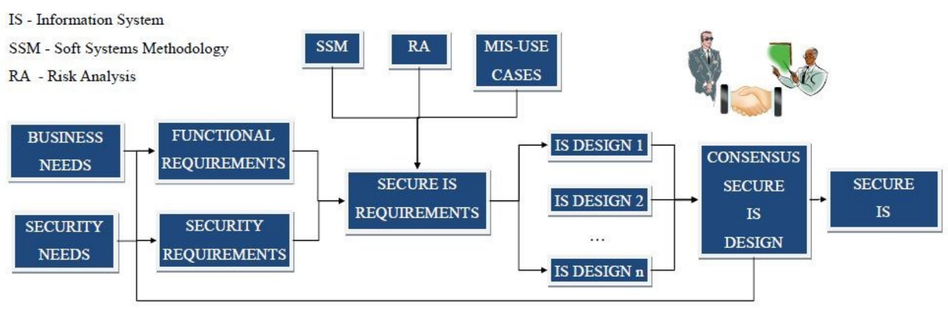
Generation	Primary Features	Means
First Generation - Checklist Methods (1972 -)	Map of limited solution onto the information problem	Survey available elements
Second Generation Mechanistic - Engineering Methods (1981 -)	A partitioned complex solution that matches functional requirements	Solve each functional requirement
Third Generation Logical-Transformational Methods (1988 -)	Highly abstracted design expressing problem and solution space	Model the essential attributes of the problem

(Baskerville, 1993)

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 complicated 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 comprises use of SSM, risk analysis and UML use case and misuse 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 consensus design.

(Cherdantseva, Poster Day, 2011)

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?

Systems Thinking — **Business Process Modelling**

The GAPS in the Existing Research

Based on the analysis conduced, four gaps in the existing research were identified:

1) There is not 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 unfeasible 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

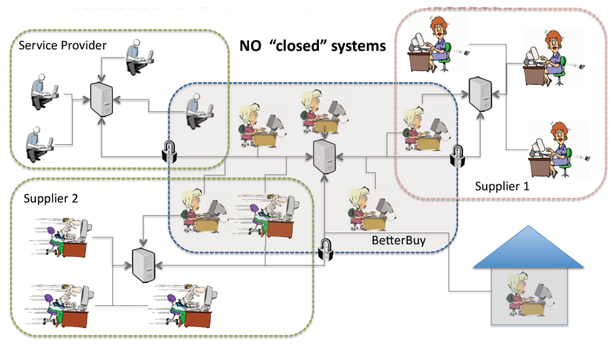
The analysis of the existing business process modelling notations and of the existing security modelling extensions allowed derivation of the requirements for the new security modelling extension. Thus, the new extension should:

- Be based on the contemporary comprehensive model of Information Security;
- Be graphical and easily understood by business experts without 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 an overall transparency, coordination and control of a complex inter-organisational process;
- Help to develop and agree consistent security policies, procedures and controls across all organisations involved into a business process;
- Help to improve level of trust between the organisations involved in information sharing.

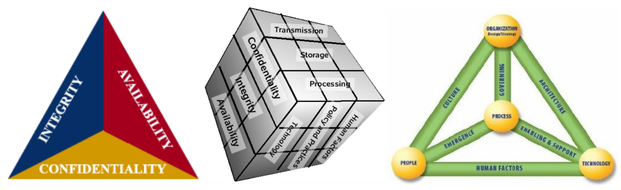
What is a *Secure* Information System? What is *Information Security* (InfoSec)?

1. The Modern Trends in InfoSec

The modern trends in InfoSec were analysed. The paper "Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success", was presented at the ISSE conference in November, 2011.



2. The Analysis of the Existing Models of InfoSec



The analysis showed the inadequacy of the models for the present interconnected environment. Moreover, the approach to InfoSec has radically changed over the last decade: InfoSec is no longer a purely technical problem, it is a problem which involves people and process, as well as legal aspects.

The development of a comprehensive contemporary model of InfoSec would be an important contribution to the discipline.

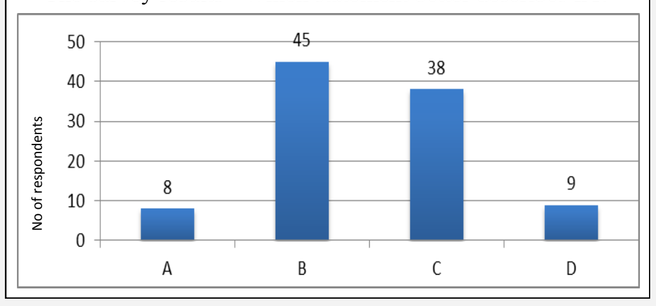
3. What is Information Assurance (IA)?

Based on the literature analysis three approaches to IA were distinguished:

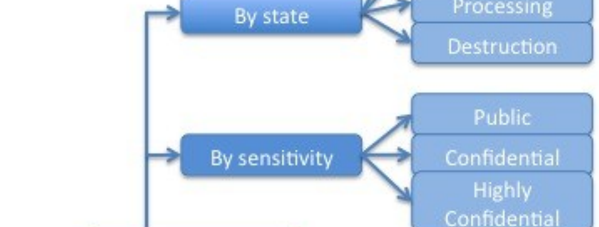
A) IA deals with the technical aspects of InfoSec;
B) IA is a holistic, multidisciplinary and systematic approach to InfoSec;
C) IA is the practice of assuring confidence in InfoSec;
D) Other.

The survey was conducted among InfoSec professionals in order to clarify the present perception of IA.

The survey results - Which statement better describes IA?



4. The Evolution of Information Security Goals



The analysis of the evolution of security goals was conducted. This analysis is important because:

- Security goals deeply characterize InfoSec at every stage of its development;
- Security goals form a fundamental part of the holistic InfoSec concept;
- Security goals serve as the evaluation criteria for Information Systems security and IT security.

The study shows that a set of security goals is not anchored; it continually changes and grows, in response to the evolution of the ICT and the society.

A Comprehensive Contemporary Model of Information Security and Information Assurance

The Future Work

The Short-term Research Aims:

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 Aims:

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.