# Aggregation of security attributes based on the granularity level of the system

Thesis Submitted in Partial Fulfilment of the Requirements for the Degree

of

## Master of Science

to the Department of Computer Science of Freie Universität Berlin

by

Artemij Voskobojnikov
Student ID: 4557770
voskobojnikov.artemij@gmail.com

First Reviewer: Prof. Dr. Jörn Eichler
First Reviewer: Prof. Dr. Marian Margraf

Berlin, <Datum>

## Affirmation of independent work

I hereby declare that I wrote this thesis myself without sources other than those indicated herein. All parts taken from published and unpublished scripts are indicated as such.

Berlin, <date>

(Artemij Voskobojnikov)

# Acronyms

# List of Figures

## Abstract

# Contents

# 1 Introduction

Security concepts can be used to capture the interacting system components, potential threats and countermeasures.

For large information systems such concepts can become very large because of the number of the involved sub-systems/components. Interconnectivity and interdepence amongst components may increase the overall system complexity and it might be therefore difficult to detect all potential impacts [1]. Methods for system abstraction that address this problem already exist. The abstraction here is the creation of representation layers which only reflect relevant properties of a system and therefore provide a better level of understanding for the respective user [8]. This for example can be achieved by different projections which reflect different granularity levels of a system displaying different levels of details [9].

In the security context such projections could be used to focus on the security or insecurity of certain sub-systems. Security attributes of components could thus be viewed separately and the security risk for a respective component could be derived. This might become especially useful when the security concept is incomplete or only partially available. An aggregation of security attributes based on the chosen projection will become possible. The system structure could then be used to derive security attributes for components that previously had none. Thus, potentially new information might become processable.

Aggregation methods for security attributes have already been suggested by researchers, e.g. transformation rules for security requirements by Menzel et al. [6] or aggregation rules for attack graphs by Noel et al. [7]. None of those methods take granularity levels or general system hierarchy into account whereas the goal of this thesis is to provide an approach which makes it possible for a user to select a sub-system of interest, i.e. a projection which reflects a certain granularity level and provides the corresponding security attributes. The relevant attributes as well as dependencies and possible aggregations will be shown to ensure an overall complete picture of the selected sub-system. This information can then be used to assess and improve the security level of the selected projection or its dependencies.

# 2 Background

Prior to addressing the actual approach and implementation some concepts and terms have to be introduced. Firstly, the term *security concept*, as it is used throughout the thesis, is being described. A definition of *granularity levels* and system abstraction follows. Lastly, a section covers *model transformations* and *aggregation rules* on security attributes.

## 2.1 Enterprise Security

To define the term *security concept* one has to look at the architecture of enterprises to understand the interconnectivity and interdependence between services, security being one of them.

### 2.1.1 Enterprise Architecture

Information systems tend to be a very complex artifacts that combine different views and requirements from various stakeholders of different backgrounds [5].

Software, IT platforms and IT related goals in general are covered in an *Information System Architecture* (ISA). ISA does not take any business-driven influences into account and is therefore insufficient when describing the complex dependencies in corporations, especially when it comes to security as described in Subsection 2.1.2.

*Enterprise Architecture Modeling* tries to overcome such possible difficulties and combines IT related concerns with business and organizational goals and shows possible interrelationships. It therefore provides an approach for an improved understanding of complex enterprise processes [10]. The Federal Deposit Insurance Corporation (FDIC) published the results of an audit of its own implementation of E-Government principles [3] and their division of information technology in Figure 1 depicts the interrelations very well.

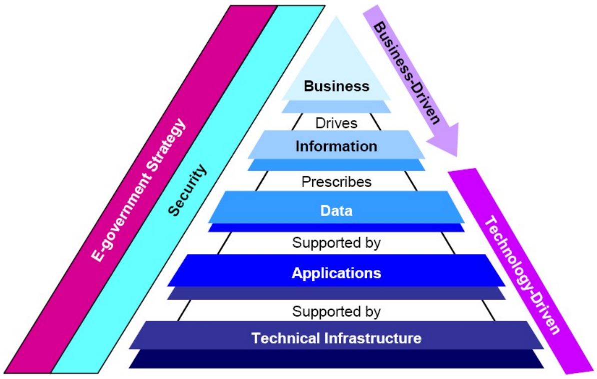

Figure 1: Division of Information Technology by FDIC

### 2.1.2 Security Architecture

Information Security has often been merely an afterthought in corporations [2] until a concept of a *Security Architecture*, published in a whitepaper by The Gartner Group [4], was introduced.

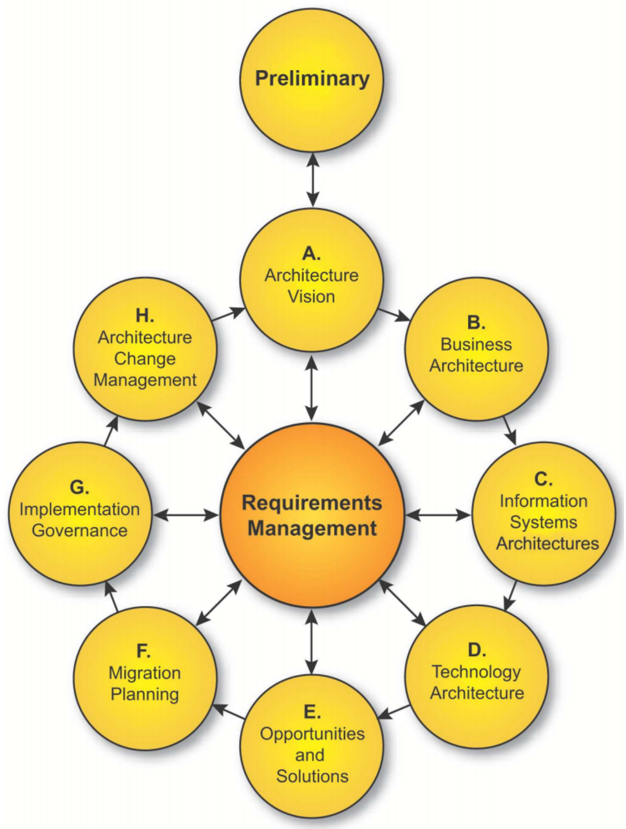
Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

Figure 2: Overview of the phases of TOGAF

#### 2.1.3 Common Criteria

#### 2.1.4 Security Concept

### 2.2 Granularity Levels

### 2.3 Model Transformation

#### 2.3.1 Aggregation rules

# References

[1] Mark Branagan, Robert Dawson, and Dennis Longley. Security risk analysis for complex systems. pages 1–12, 2006.

[2] Edwin Covert. Using enterprise security architectures to align business goals and it security within an organization. http://www.ansfederal.com/, 2010.

[3] FDIC. Implementation of e-government principles.

[4] Gregg Kreizman and Bruce Robertson. Incorporating security into the enterprise architecture process. *Gartner Research*, 2006.

[5] Stephan Kurpjuweit and Robert Winter. Viewpoint-based meta model engineering. In Manfred Reichert, Stefan Strecker, and Klaus Turowski, editors, *Enterprise Modelling and Information Systems Architectures - Concepts and Applications, Proceedings of the 2nd Int'l Workshop EMISA 2007*, volume P-119, pages 143–161, Bonn, Oktober 2007. Gesellschaft für Informatik, Köllen.

[6] Michael Menzel, Christian Wolter, and Christoph Meinel. *Towards the Aggregation of Security Requirements in Cross-Organisational Service Compositions*, pages 297–308. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[7] Steven Noel and Sushil Jajodia. Managing attack graph complexity through visual hierarchical aggregation. In *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, VizSEC/DMSEC '04, pages 109–118, New York, NY, USA, 2004. ACM.

[8] Klaus Pohl, Harald Hönninger, Reinhold Achatz, and Manfred Broy. *Model-Based Engineering of Embedded Systems: The SPES 2020 Methodology*. Springer Publishing Company, Incorporated, 2012.

[9] Judith Thyssen, Daniel Ratiu, Wolfgang Schwitzer, Alexander Harhurin, Martin Feilkas, and Eike Thaden. A system for seamless abstraction layers for model-based development of embedded software. In *Software Engineering (Workshops)*, pages 137–148, 2010.

[10] R. Winter and R. Fischer. Essential layers, artifacts, and dependencies of enterprise architecture. In *2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06)*, pages 30–30, Oct 2006.