



# 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 Voskobochnikov

Student ID: 4557770

voskobochnikov.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 All parts taken from published and unpublished scripts are indicated as such.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 Voskobjnikov)

## Acronyms

## List of Figures

|    |  |    |
|----|--|----|
| 1  | Four acts that cause security harm . . . . .             | 3  |
| 2  | ISMS Stakeholder Concerns . . . . .                      | 5  |
| 3  | Overview of the Security Target contents . . . . .       | 7  |
| 4  | Relationships between Model and Metamodel . . . . .      | 10 |
| 5  | Model transformation according to Jouault et al. . . . . | 11 |
| 6  | Model transformation . . . . .                           | 12 |
| 7  | Security Concept Metamodel . . . . .                     | 17 |
| 8  | Two different interpretations of data . . . . .          | 18 |
| 9  | Structural information . . . . .                         | 19 |
| 10 | Attributes of a Security Goal . . . . .                  | 23 |
| 11 | Relationships between Security Goals . . . . .           | 23 |
| 12 | Ambiguous propagation . . . . .                          | 24 |
| 13 | Ambiguous propagation . . . . .                          | 25 |
| 14 | Attributes of a Threat . . . . .                         | 26 |
| 15 | Underspecified Security Concept with a Threat . . . . .  | 27 |
| 16 | Underspecified Security Concept with a Control . . . . . | 29 |

## Abstract

# Contents

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Introduction</b>   | <b>1</b>  |
| <b>2</b> | <b>Background</b>   | <b>2</b>  |
| 2.1      | Security . . . . .  | 2         |
| 2.1.1    | Security Architecture . . . . .                               | 4         |
| 2.1.2    | Common Criteria . . . . .                                     | 6         |
| 2.1.3    | Security Concept . . . . .                                    | 8         |
| 2.2      | Modeling . . . . .  | 8         |
| 2.2.1    | Model Transformation . . . . .                                | 10        |
| 2.2.2    | Granularity Levels . . . . .                                  | 12        |
| <b>3</b> | <b>Related Work</b>   | <b>13</b> |
| 3.1      | Granularity layers . . . . .                                  | 13        |
| 3.2      | Security Attribute Aggregation . . . . .                      | 14        |
| 3.3      | Validation of Model Transformations . . . . .                 | 16        |
| <b>4</b> | <b>Approach</b>   | <b>16</b> |
| 4.1      | Security Concept . . . . .                                    | 17        |
| 4.2      | Metamodel elements and their security properties . . . . .    | 19        |
| 4.2.1    | Components . . . . .  | 19        |
| 4.2.2    | Data . . . . .  | 20        |
| 4.2.3    | Interpretation of Interconnections between Elements . . . . . | 22        |
| 4.3      | Model Transformation . . . . .                                | 29        |
| 4.4      | Transformation Rule Set for Security Goals . . . . .          | 31        |
| 4.4.1    | Aggregation Rules . . . . .                                   | 31        |
| 4.5      | Transformation Rule Set for Threats . . . . .                 | 31        |
| 4.5.1    | Aggregation Rules . . . . .                                   | 31        |
| 4.6      | Transformation Rule Set for Controls . . . . .                | 31        |
| 4.6.1    | Aggregation Rules . . . . .                                   | 31        |
| <b>5</b> | <b>Implementation</b>   | <b>31</b> |
| 5.1      | Technology . . . . .  | 31        |
| 5.2      | Validity & Verification . . . . .                             | 31        |
| 5.3      | Runtime & Complexity . . . . .                                | 31        |
| <b>6</b> | <b>Summary</b>  | <b>31</b> |
| <b>7</b> | <b>Outlook</b>  | <b>31</b> |

# 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 interdependence amongst components may increase the overall system complexity and it might be therefore difficult to detect all potential impacts [2]. 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 [15]. This for example can be achieved by different projections which reflect different granularity levels of a system displaying different levels of details [19].

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. [10] or aggregation rules for attack graphs by Noel et al. [12]. 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 Security

Morrie Gasser [4] published a book in 1988 providing solutions for computer specialists interested in computer security. The term *Computer Security* usually dealt with three aspects:

- Prevention of theft or damage to the hardware
- Prevention of theft or damage to the information
- Prevention of service disruption

With the invention of the Internet the (personal) computers got interconnected and the sharing of data became prevalent and thus data security.

Nowadays security is seen as a process. No combination of products are guaranteed to make a system secure since they are only as secure as the people configuring them [21].

In general when talking about computer security three aspects are addressed, *Confidentiality*, *Integrity* and *Availability* [14]. Each of them will now be defined:

**Confidentiality** Assets can only be accessed by authorized parties

**Integrity** Assets can only be modified by authorized parties

**Availability** Assets are available to authorized parties when needed

The challenge is seen in finding the right balance between the three *Security Goals*. This situation is aggravated by the fact that the goals can overlap, be independent or even mutually exclusive. Charles P. Pfleeger [14] for example, addresses this problem by stating that a strong protection of confidentiality might restrict availability in a system.

Information systems consist of hardware, software and data and it is of high importance for the respective stakeholder to secure the object of interest.



When speaking about securing systems or components we look at two different terminologies, *Vulnerabilities* and *Threats*. A *vulnerability* is a system weakness, be it in implementation or design, that can be potentially exploited by an adversary. Without the intent of exploiting it the vulnerability has no further effect on the system.

A *threat* however is a set of circumstances that has the theoretical potential to cause harm by exploiting a specific vulnerability [21]. An example to demonstrate the differences follows:

**Vulnerability:** Sending sensitive data over an unsecured channel

**Threat:** Exploiting the unsecured channel by eavesdropping and gathering the sensitive data

As mentioned before a system weakness does not necessarily mean loss of data or any other system breach. Only when coupled with a set of circumstances and the intent of exploitation it turns into a threat. Figure 1 illustrates the four acts that cause security harm as mentioned by Pfleeger [14].

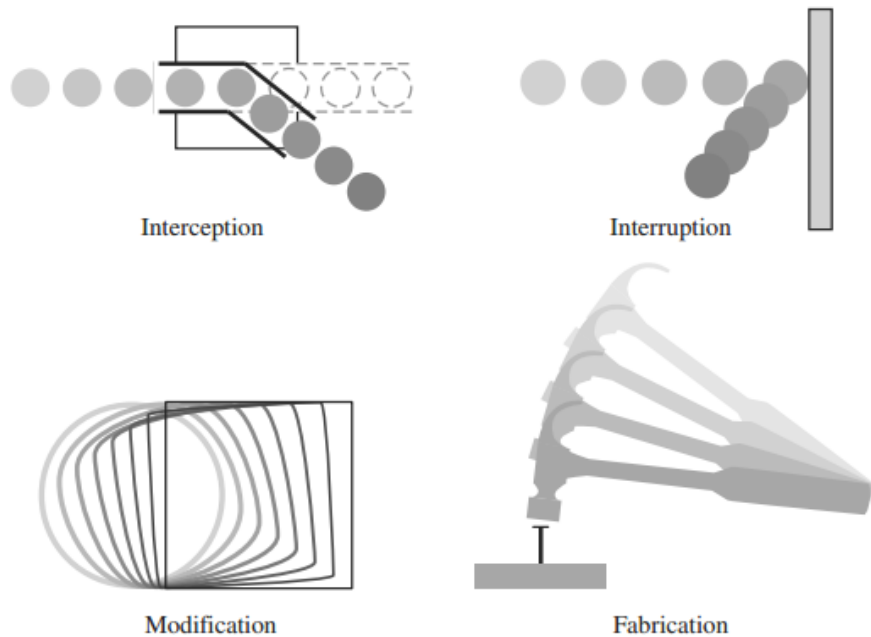


Figure 1: Four acts that cause security harm

Confidentiality, integrity and availability, or the C-I-A triad like it is also being called, can be viewed from a perspective of the causes of harm. Confidentiality can suffer if some unauthorized party intercepts the data, availability

can be lost if a flow of data is being interrupted and lastly integrity can be broken if the data is being modified or false data is being fabricated by an adversary.

To prevent the vulnerabilities from being exploited and the threats from potentially causing harm one can use *Controls* or *Countermeasures* to secure parts of a system. An example would be the use of encryption to prevent sensitive data from being eavesdropped on as mentioned in 2.1.

To put everything into perspective the term *Security Architecture* will be introduced.

### 2.1.1 Security Architecture

Gacek et al. discussed the definition of a *Software System Architecture* (SSA) which will be used and adapted in the security context. According to the authors a *Software System Architecture* is:

- A collection of software and system components, connections and constraints
- A collection of system stakeholders' need statements
- A rationale which demonstrates that the elements which define a system satisfy the the stakeholders' needs, if implemented correctly

Here, a *Security Architecture* (SA) would be an adapted definition where, if implemented correctly, the stakerholders' *security* needs will be satisfied. Naturally, the connections as well as the respective components might differ from the Software System Architecture as they might have to be enhanced or altered to satisfy the security needs.

The stakeholders themselves however, are very similar. Gacek et al. differentiate between five parties, the *Customer*, the *User*, the *Architect and System Engineer*, the *Developer* and the *Maintainer*.

The International Standard ISO 27001 provides a model for establishing, impelementing, operating, monitoring, reviewing, maintaining and improving an organization's Information Security Management System [1], i.e. a system that is responsible for establishing and maintaining organization's security needs and guidelines. When comparing these rather short definitions one can already see an overlap when looking at potential stakeholders. An overview on the SSA stakeholders follows:

| Stakeholder                   | SSA Concern  |
|-------------------------------|--|
| Customer                      | Schedule and budget estimation<br>Feasibility and risk assessment<br>Requirements traceability<br>Progress tracking                        |
| User                          | Consistency with requirements and usage scenarios<br>Future requirement growth accommodation<br>Performance, reliability, interoperability |
| Architect and System Engineer | Requirements traceability<br>Support of tradeoff analyses<br>Completeness, consistency of architecture                                     |
| Developer                     | Sufficient detail for design<br>Reference for selecting/assembling components<br>Maintain interoperability with existing systems           |
| Maintainer                    | Guidance on software modification<br>Guidance on architecture evolution<br>Maintain interoperability with existing systems                 |

When looking into the International Standard, one can see that similar concerns can be also found in the adaptation of the „Plan-Do-Check-Act“ model for the establishment of an ISMS process. In the case of ISMS similar aspects can be found in the four different phases as seen in Figure 2.

|  |   |
|--|---|
| <b>Plan (establish the ISMS)</b>           | Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives. |
| <b>Do (implement and operate the ISMS)</b> | Implement and operate the ISMS policy, controls, processes and procedures.  |
| <b>Check (monitor and review the ISMS)</b> | Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.   |
| <b>Act (maintain and improve the ISMS)</b> | Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.                        |

Figure 2: ISMS Stakeholder Concerns

Security requirements and objectives have to be defined in the earlier phases so they can be planned, implemented and carried out by the respective security architects/developers/security engineers. Here, the term user is not as clear since a variety of employees can be seen as such, e.g. any employee that accepts the established security policies. Since systems, as mentioned

in Section 2.1, are just as secure as the people using them, many employees can be viewed as ISMS users. They would be interested in implementing and operating the processes and procedures which have been defined in the previous phase.

Established security policies have to be also monitored and maintained. Security is never guaranteed and is a complex process [21] - systems have to be constantly updated and possibly upgraded.

A Security Architecture is therefore a union of security objectives by different stakeholders and, if properly implemented, guarantees the stakeholders' needs. These needs have to be considered throughout the system processes and have to be registered in a comprehensible manner. Security requirements have been mentioned and, amongst others, will be described more thoroughly in the next section.

### **2.1.2 Common Criteria**

The following section will present a way of modeling security concerns for an asset of interest.

Common Criteria proposes an evaluation by using a so called *Security Target* (ST), a construct that encapsulates the *Target of Evaluation* (TOE), threats to the TOE and countermeasures [18]. The goal of the evaluation is to show that the used countermeasures are sufficient to counter potential threats and thus implying that the TOE is sufficiently protected.



Figure 3: Overview of the Security Target contents

A description of all the contents of a ST is unnecessary here and only the key security attributes of a ST that will be used to construct a *Security Concept* (Subsection 2.1.3) are being introduced.

The *Security Problem Definition* defines, as the name suggests, the security problem that is being addressed. Apart from containing guidelines and assumptions it contains *Threats* which are „[...] *adverse actions performed by a threat agent on an asset*“ ([1], p. 66).

A *Security Objective* is an abstract solution to the previously defined security problem. There exists a possibility to divide the *Security Objectives* into part wise solutions, one being the *Security Objectives for the TOE* and the other being the *Security Objectives for the Operational Environment*. Moreover does the ST contain traces showing which objectives address which threats, guidelines and assumptions and a set showing that all threats, guidelines and assumptions are addressed by the security objective.

*Security Functional Requirements* (SFR) are a more detailed translation of the previously defined *Security Objective*. Despite being more detailed, SFR

have to be still independent from specific technical solutions. Lastly, STs contain a TOE summary specification where it is stated how the TOE meets all the SFRs and how exactly those requirements are met on a technical level.

### 2.1.3 Security Concept

The term *Security Concept*, as it is defined here, is based on the constructs introduced in the previous chapters, namely *Security Architecture* and *Security Target*. An overview follows.

*Assets* are the to be secured objects of interest, i.e. TOE according to Common Criteria. *Assets* can be either logical or physical and can be grouped to sets, if needed.

A *Security Goal* (SG) is the equivalent to the *Security Objective*. A valid SG must address an *Asset* and a *Security Goal Class* that defines the actual purpose of the SG. In general the set of *Security Goal Classes* consists of *Confidentiality*, *Integrity* and *Availability* but can also be expanded by further classes such as *Authenticity*.

*Threats* serve the same purpose as proposed by Common Criteria. They are adverse actions performed by an entity against an *Asset*.

This information is all brought together in *Security Requirements* that are defined in natural language and show the interrelationships between elements. A *Security Goal* has to be mentioned as well as an *Asset* and a *Threat* against which the object of interest should be protected.

Lastly, *Controls* are the technical measures that counter or minimize the *Threats*.

The Table 1 depicts the relationships between all the security attributes:

## 2.2 Modeling

To ensure a viable solution one has to think of a representation of real life systems. *Models* can be used to achieve this by depicting the key properties and processes of a certain system. According to Ed Seidewitz [17] a model is a „*set of statements about some system under study*“ with the statements being either correct or incorrect.

A system modeled using the Unified Modeling Language (UML) serves as an example. In this case such statements could be made on the relationships between classes and would only be correct if they are consistent with the actual structure of the respective system under study (SUS), i.e. the described (modeled) relationships do indeed exist.

| Name                 | Contains                     | Description   | Example  |
|----------------------|------------------------------|---|--|
| Asset                | -                            | Digital or physical object of interest that should be secured | Sensible user data   |
| Security Goal Class  | -                            | Defines the purpose of the Security Goal                      | Confidentiality of sensible user data  |
| Security Goal        | Security Goal Class, Asset   | Defines the security objective                                | Confidentiality of sensible user data shall be protected                           |
| Threat               | Asset                        | Adverse action against an Asset                               | Eavesdropping on sensible user data  |
| Security Requirement | Asset, Security Goal, Threat | Security Objective in natural language                        | The Confidentiality of sensible user data shall be protected against eavesdropping |
| Control              | Threat                       | Measure to minimize or mitigate the Threat                    | Encryption of sensible user data with AES-256 to prevent eavesdropping             |

Table 1: Elements of a Security Concept

In our case we would try to create a model that reflects the security attributes and their interrelationships in a SUS. This interpretation of a model is key because only then the model is given a meaning [17].

A definition of a model is not enough. A *metamodel* has to be clearly defined to verify whether a model is conform or not, i.e. whether a security concept instance is conform to its security concept metamodel. The following figure shows the interrelationships.



Figure 4: Relationships between Model and Metamodel

A security concept of a SUS would be modeled in a modeling language, e.g. UML which is a representation of its own metamodel. At the same time the security concept would be conform to its metamodel. This conformity, be it the security concept or the modeling language, is needed for a model to be considered valid.

### 2.2.1 Model Transformation

The Meta Object Facility (MOF) [13] is a standard metamodel proposed by the Object Management Group (OMG) and captures the relationships between models in a three-layered architecture consisting of M1, M2 and M3. Models (M1) are representations of systems and are expressed in a modeling language M2, e.g. UML as mentioned in the previous section, which is conform to a so called metamodel. Metamodels themselves are also expressed in a metamodeling language which is conform to a metamodel (M3).



These architecture levels can be found in the *model transformation pattern* by Jouault et al. [5] which can be seen in Figure 5.



Figure 5: Model transformation according to Jouault et al.

Here a source model  $Ma$  is being transformed into a target model  $Mb$  using a transformation language. Both models and the transformation language are conform to their respective metamodel which is the traditional understanding of a model transformation.

Kleppe et al. defined a *transformation* as an automatic generation of a target model from a source model according to *transformation rules* that describe how elements from the source model can be transformed into a target model [7].

This transformation may have different levels of automation. An *automatic* transformation would not need any manual intervention from the user. In cases where incompleteness or inconsistencies may occur a manual intervention may be needed [9].

Throughout the introduction and the background chapter the derivation of security attributes based on structural properties of a system of interest was mentioned. Given a model  $M$  this derivation can be seen as alteration of  $M$  and therefore as a *model transformation*. The resulting model  $M'$  is different

to  $M$ , both however, are conform to the same metamodel  $MM$  whereas  $MM$  is conform to  $MMM$ . In our case both source and target languages are identical. We can therefore simplify the transformation graph shown in Figure 5.

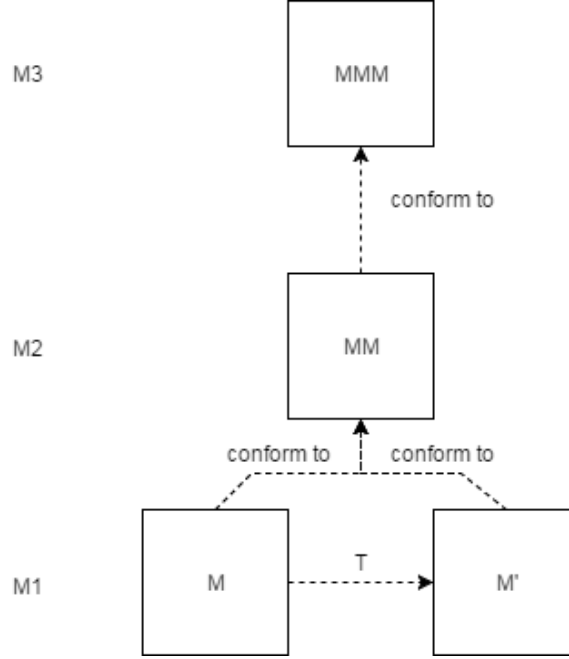


Figure 6: Model transformation

The definition of a transformation  $T$ , or better a *transformation rule set*, that alters a model  $M$  is the main goal of this thesis.

Prior to the actual rule set definition one final concept has to be introduced. A user-selected *Granularity level* serves as a second input in the model transformation. The transformation itself should be automatic, the only user input should be the just mentioned granularity level.

### 2.2.2 Granularity Levels

Information systems are often complex because of the number of interconnections and interdependencies between components and therefore it might be difficult to assess potential impacts and risks of a system [2].

One logical goal would be to decrease the overall complexity to enable a better risk assessment. *System abstraction* tries to achieve this by reducing the level of details [2]. Thyssen et al. differentiate between two possibilities, *Whole-part decomposition* which decomposes a system into smaller sub-systems and

*Distinct development perspectives* which focuses on certain parts of a system depending on the current development perspective.

In this thesis the focus will be on the *Whole-part decomposition* even though an adaption of development perspectives is certainly possible. The main difficulty would be the definition of such perspectives in the security context because they would be highly dependent on the respective security analyst. The perspectives would not be unambiguous.

Therefore the change of the level of detail, i.e. the granularity level, will be achieved by uniting or decomposing components of a system of interest. By decomposing a larger system into smaller sub-systems one could focus on only specific security attributes and dismiss others.

A user will select a certain granularity level, i.e. a certain set of components, as an input to the transformation function  $T$  as mentioned in 2.2.1. Together with the defined rule set a valid model  $M'$  will be generated which to be considered valid has to conform to its metamodel  $MM$ .

## 3 Related Work

Several publications that provide an essential basis for this thesis will now be presented. A variety of different topics will be briefly covered such as abstraction layers/granularity layers, security attribute aggregation and propagation as well as model transformations and formal verification.

### 3.1 Granularity layers

Thyssen et al. presented a framework which allowed them to view models under different levels of abstraction [19]. This abstraction is achieved by introducing granularity levels which are based on the different needs of the stakeholders.

Two different approaches were suggested where one is *Whole-part decomposition* which applies the divide-and-conquer principle and decomposes the SUS into smaller blocks until atomic blocks are reached. The other possible method is viewing the system from *Distinct development perspectives*. The differences have already been briefly discussed in Section 2.2.2 and therefore only whole-part decomposition will be presented in more detail.

Thyssen et al. propose a decomposition of systems into sub-systems to overcome the complexity. A sub-system is seen as an independent system by itself and the goal is to achieve „seamless“ abstraction. This way the sub-systems could be viewed separately and, if needed, could be aggregated to the overall system.

Different development perspectives were also proposed to focus on specific stakeholders and their needs during the system abstraction.

The *user perspective* describes, as the name suggests, the user's interests and the fulfilment of such by the respective system. The focus is on the hierarchical structuring of the general system functionality based on the users' needs and the functional interrelationships between components. The *logical perspective* can be seen as a bridge between the user-defined requirements and the technical implementation and lastly, the *technical perspective* describes the technical side, i.e. the hardware components that incorporate the needs of the respective users.

In this thesis however, the main focus is the combination of the security perspective and the „seamless“ abstraction of systems. As previously mentioned security in information systems is seen as a complex process [21] and the realization of security policies may have effects on different perspectives. Throughout the thesis system abstraction will be addressed from the perspective of a security architect that tries to incorporate all the stakeholders' security needs in a system. The goal is to propose a solution on how security properties of systems propagate through different levels of abstraction. Dependencies amongst them have to be taken into account and appropriate aggregation rules have to be defined.

Thyssen et al. have introduced the theoretical idea of „seamless“ abstraction but have not addressed the transformation steps that are needed to transform a system from one granularity level to another.

### 3.2 Security Attribute Aggregation

Aggregation of security attributes has been studied and aggregation rules have been discussed by multiple researchers. Menzel et al. focused on the aggregation of security requirements and dependencies amongst them [10]. They defined interaction sets for requirements that classified the effects two requirements  $r_1$  and  $r_2$  might have on each other. According to [10] requirements could be independent, equivalent or conflicting, just to name a few.

Furthermore, when addressing the actual aggregation, Menzel et al. argued that to propose correct rules one has to look at two core aspects. Firstly one has to determine whether two requirements belong to the same class of security goals or not and secondly, the addressed entities and dependencies amongst the requirements have to be considered.

The transformation rules, which will be defined in Section 4, use this concept as the basis. Even though Menzel et al. have not addressed the needed transformation steps they provided core aspects that are essential for the aggregation of requirements. These will also be considered during application

for different security attributes.

Similarities can be found when looking at the work carried out by Noel et al. [12] which addresses attack graph aggregation.

Attack graphs are a representation of possible vulnerabilities in a network that can be exploited by attackers. Interactions and dependencies are represented by edges and for large networks such graphs may become very complex. To reduce the just mentioned complexity rules have been introduced that hierarchically aggregate graph elements.

Rules for exploits and security conditions, i.e. states that exist prior to or after an exploit, have been proposed. Exploits are being aggregated based on the attacker/victim machines where only exploits on the same machines are being aggregated into exploit sets.

Conditions are being aggregated into condition sets when they are either preconditions or postconditions of the same exploit. Later on, an aggregation based on machine level is being executed, i.e. conditions are being aggregated if they all occur on the respective machine. A machine is therefore a union of all its conditions.

Both the idea of aggregation based on same elements/machines as well as the idea of union sets consisting of conditions will be adapted in this thesis. Lastly, risk aggregation is being covered. Lenstra et al. [8] have discussed both the qualitative as well as the quantitative risk analysis providing both the advantages and disadvantages of the respective method. Qualitative risk analysis assigns subjective values to risks or threats (such as High, Medium or Low) and these values then display the severity of the respective threat or risk. Qualitative approaches however, only provide very vague indications which might not be suitable for specific, more complex systems.

Quantitative approaches view the underlying events as distribution functions and derive the overall risk of an element from said functions. As mentioned by Lestra et al. and example could be the *Annual Loss Expectancy* for an event which can then be aggregated when viewing different events.

In our case quantitative aggregation is not necessary and might not even be possible in many cases since the given security concepts might be underspecified.

Our goal is to provide a solution on security attribute propagation for as many systems as possible applying qualitative aggregation for security attributes defined in the metamodel in Section 4.1. Although it is less precise than quantitative approaches [8] it suffices when considering the possibility of underspecification of security concepts and the overhead during aggregation steps when applying such an analysis.

### 3.3 Validation of Model Transformations

When proposing the model transformation one has to determine its correctness. Varro et al. define four properties that verify the correctness of a model transformation [21].

**Syntactic correctness:** The generated model is a syntactically correct model instance (is conform to its metamodel)

**Termination:** Model transformations must terminate

**Uniqueness:** Model transformations must be deterministic

The fourth criterion is the *semantic correctness* which usually implies a semantic equivalence between source and target model. Here however, the model transformation is a projection, i.e. a possible gain/loss of information is possible.

Oracle functions serve the purpose of validating a model transformation output. The definition of such may become very difficult because of the complex nature of models as data structures [11]. Model comparison is described as one possible solution to validate a model transformation. Mottu et al. introduce a general oracle containing six different functions validating a given test case. Our primary goal however is the semantic gain of the projection and to verify this we have to define a very specific oracle in the security context. Model verification through testing is the most common form of validation [3] and thus, we will provide an implementation of the transformation rules and will validate its results by testing with sample models as inputs. The purpose of the testing process is the *detection of errors in the implementation*, the *completion of the specification* and lastly the *assessment of the result*, as mentioned by Fleurey et al.

The most important aspect is the result assessment. In our case the satisfaction highly depends on the respective user (e.g. security engineer) and we therefore have to define a criterion which reflects a successful model transformation of the initial security concept while being independent of the user. The approach will be an oracle based on model comparison and will be discussed in Section 5.2.

## 4 Approach

This section presents the approach addressing the previously mentioned goal of a model transformation based on the user-selected granularity level of a

The second part will deal with the actual transformation rules. Model transformations will be mathematically defined and the transformation rules for each element of the model will follow. Aside from the solution possible edge cases will be presented and evaluated.

The following metamodel is based on the security elements mentioned in Section 2.1.3. It shows the interconnections between elements and adds restrictions. This metamodel serves as a base enabling the creation of model instances capturing the relations between components/assets of a specific SUS. It also provides a security context and the option for the user to select a granularity level.



17

*Threat* are pictured. All of these elements are part of a *SecurityConcept*, which in this model will be simply identified by a name.

SGs have a *Security Goal Class* attribute which describes the purpose of each SG. The *Damage Potential* attribute indicates at the importance of a Goal, i.e. how important it is to secure a certain asset. The higher the damage potential the higher the impact if the security of an asset is breached. One key aspect of this metamodel is the dependency between SGs. A SG is dependent on another SG if both belong to the same asset and have the same security goal class. These dependencies, amongst others, have to be considered during potential transformation steps (Section 7).

Each SG belongs to exactly one asset whereas an asset itself can have unlimited SGs. In this thesis both physical and virtual components can be considered an asset. Both *Data* and *Component* can be assets according to the metamodel.

There will be two different types of data. For once *processed data*, i.e. data that is being processed or kept in storage by a specific component. On top of that *transmitted data* will be considered separately since the transmission channel itself can be seen as an asset. The resulting interconnections are shown in the following figure:

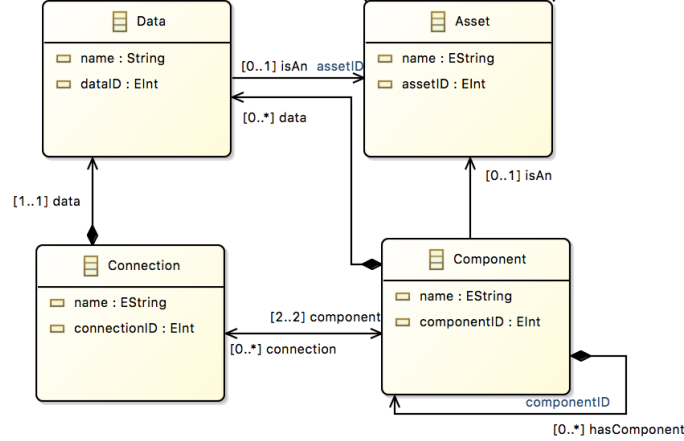


Figure 8: Two different interpretations of data

As already mentioned data can be viewed as being processed and transmitted. Therefore an element *Connection* was added. A connection is the transmission channel between two components. It must have an associated data. The processed or stored data however can be directly associated with a component. In both cases data can be viewed as an asset. There is no possibility to assign a connection as an asset, the reason being that the transmission



medium itself, i.e. the cable, wire, is rarely an object of interest but more so the data which is being transmitted.

Lastly the selection of *Granularity Levels* by users should be enabled. Instead of having two different input models, one security concept model and one model depicting the system structure, one can reproduce the structural properties by adding a reference to the component element.

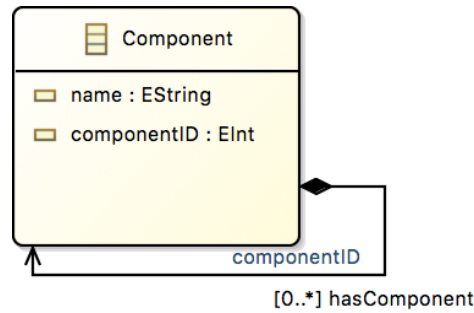


Figure 9: Structural information

Having this extra reference one can create infinitely deep structural dependencies within the model. Therefore the actual transformation will only require one model instead of two separate ones.

## 4.2 Metamodel elements and their security properties

To put the different elements of the metamodel into a security context one has to clearly define the Security Goal Classes for possible assets. Interpretations of the classes are not unambiguous and it is necessary to discuss how security attributes propagate through different abstraction layers and what kind of impact interrelated components on different layers have on each other.

### 4.2.1 Components

Before introducing the transformation rules one has to look at the different kinds of components that can be potentially found in a model instance. Even though the model element remains the same (*Component*) a distinction which is made here is necessary because the interpretation of Security Goal Classes differs depending on the component type.

#### Physical Component

Physical components are components that can be accessed physically, e.g. computers, servers, switches etc. Since those can be accessed physically

and therefore be manipulated physically one has to define the Security Goal Classes accordingly.

1. **Confidentiality** - Will be *undefined* for physical components and will only hold for data stored/processed on those components
2. **Integrity** - Ensured when the component has not been altered by an adversary in any way; can be broken by an adversary having physical access
3. **Availability** - Ensured when the component is able to carry out its designated task; can be broken by an adversary having physical access

### Virtual Component

Virtual components cannot be directly accessed physically. Examples would be virtual machines, virtual switches etc. The classes are similar to the physical counterpart except from the breach of the respective class.

1. **Confidentiality** - Will be *undefined* for virtual components and will only hold for data stored/processed on those components
2. **Integrity** - Ensured when the component has not been altered by an adversary in any way; can be broken remotely by an adversary, i.e. without having physical access
3. **Availability** - Ensured when the component is able to carry out its designated task; can be broken remotely by an adversary, i.e. without having physical access

#### 4.2.2 Data

Similar to the component element the data element can be interpreted in different ways. The distinctions between the different data types are very minor but noteworthy nonetheless. We consider three types of data, data which is being stored by a component, data which is being processed by a component and data which is being transmitted between components. The common terminology is *Data at Rest*, *Data in Motion* and *Data in Use* [6]. The used terms might be new, the distinction between different states of data however can be found in publications going as far back as 1982, e.g. by Dorothy E. Denning [16].

## Data at Rest

Data at Rest applies to devices that hold data [6]. An example would be a database containing sensitive information. The database being the *Virtual Component* and the stored data being the *Data at Rest*. One could also define the server with the database as a *Physical Component*.

1. **Confidentiality** - Ensured when the data is protected from unauthorized disclosure at rest
2. **Integrity** - Ensured when the data is protected from unauthorized modification at rest
3. **Availability** - Ensured when the data is available to authorized parties when needed, i.e. authorized parties can access and use the data when needed

## Data in Use

Data in Use applies to data that is being processed by a component, i.e. is being used by a service running on a component. An example would be data that is being processed by an API on a server. The API being the *Virtual Component* and the server being the *Physical Component*. The *Data in Use* would be the processed information by the API backend.

1. **Confidentiality** - Ensured when the data is protected from unauthorized disclosure during processing
2. **Integrity** - Ensured when the data is protected from unauthorized modification during processing
3. **Availability** - Ensured when the data is available to authorized parties when needed, i.e. the data is being processed by the service/the respective service is running when needed

## Data in Motion

Data in Motion applies to all data transmitted between components. We do not specify any protocols here to keep the definition as broad as possible.

1. **Confidentiality** - Ensured when the data is protected from unauthorized disclosure during transmission

2. **Integrity** - Ensured when the data is protected from unauthorized modification during transmission
3. **Availability** - Ensured when the data is available to authorized parties when needed, i.e. is not lost or intercepted during transmission

The different component/data types shown here should only show the different interpretations of the elements of the security concept metamodel. The interpretation of the element itself does not have an influence on the chosen metamodel element, i.e. the element for both physical and virtual components will still be *Component*. The only difference can be found in data since transmitted data always belongs to a *Connection*. For both processed and stored data however the metamodel element *Data* will be used.

#### 4.2.3 Interpretation of Interconnections between Elements

To describe model transformations in the security context one has to discuss how exactly the security attributes propagate through the respective abstraction layers. Here we will look into the dependencies between components and their security properties during transformations.

##### Sub-component

A sub-component *SC* will be defined as a component that directly belongs to a component *C* which is in an abstraction layer above, i.e. encapsulates one or more sub-components. According to the previously defined metamodel such a relationship between components is being defined by the *hasComponent* composition, i.e. a sub-component cannot exist without a component here. This also means that no new data types or structures are added when changing to higher granularity levels. Sub-components can only process data that has already been defined in the layers above. An example would be a database encapsulating a sub-component such as a secure key storage.

##### Security Goals

For security goals the interconnections between components and sub-components have to be interpreted in an unambiguous way. There is no clear definition on how SGs for components in higher abstraction layers propagate to the respective sub-components in the abstraction layers below. We therefore adopt the idea for security requirements which was proposed by Menzel et al. [10]. Here, the main focus will be on two characteristics, *Independent* and

*Require* to capture interdependencies between SGs on different granularity levels. According to the metamodel each SG has the following attributes:

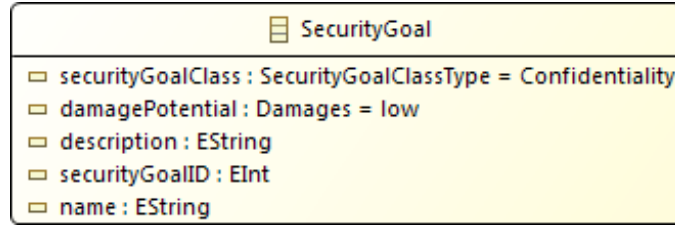


Figure 10: Attributes of a Security Goal

The key attributes are *securityGoalClass* and *damagePotential*. Both are relevant when it comes to aggregation rules and dependencies amongst components. In this chapter the focus will be on the latter.

In case of a complete security concept definition interdependencies amongst components and security goals are clear, similar to Figure 11. Out of simplicity security goals will be linked directly to components and not through assets.

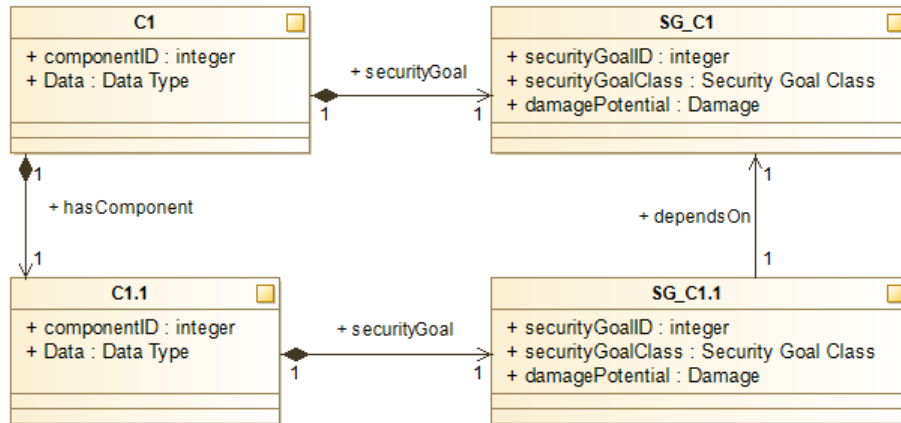


Figure 11: Relationships between Security Goals

Figure 11 has shown the dependencies between components and their security attributes in case of a complete security concept definition. In underspecified security concepts, such as shown in Figure 13, the dependencies are not as trivial.

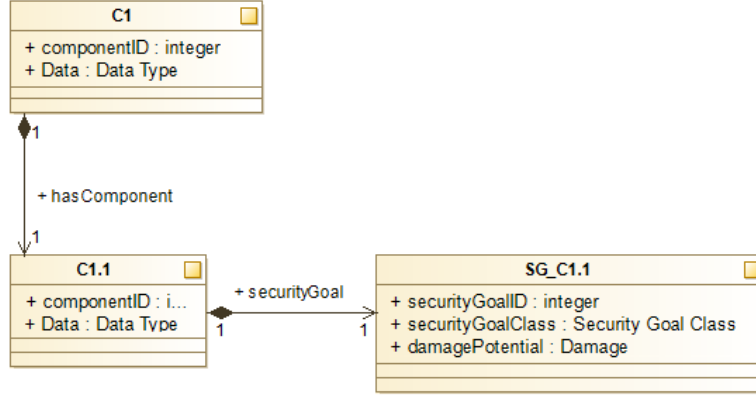


Figure 12: Ambiguous propagation

It is not obvious what kind of influence the sub-component has on its parental node, if at all. If the confidentiality of component  $C_{1.1}$  is protected it is not clear how it will propagate to higher abstraction layers. Similar observations can be made for the aggregation from higher abstraction layers to lower ones. One has therefore to define when and how security attributes will propagate based on structural features of the SUS.

**Definition 1** *A security goal  $SG_{C_1}$  of a component  $C_1$  has a direct influence on another component  $C_2$  if and only if there is:*

1. *a direct link between the two components, i.e. a hierarchical relationship between the two components AND*
2. *component  $C_2$  processes/holds the data type that is being addressed by  $SG_{C_1}$*

This *direct influence* is one of the more obvious dependencies amongst components. At first glance matching data types are needed to aggregate SGs through different abstraction layers but it is certainly possible that security concepts might be underspecified. Relying on this definition might therefore severely limit the transformation and thus, the resulting model.

An exemplary model instance follows showing security attribute propagation with an underspecified security concept. Similarly to previous examples data/components will be directly linked with security goals without asset elements in between in the interest of greater clarity.

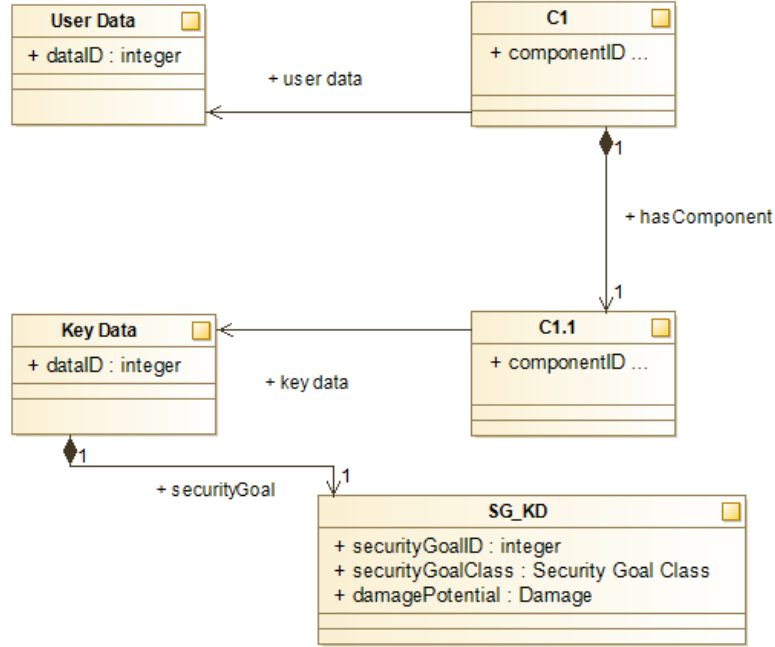


Figure 13: Ambiguous propagation

The corresponding security goal of the key data in natural text could be:

$SG_{KD}$  : The Confidentiality of sensible key data should be protected

Now we will look at component  $C_{1.1}$  which has a link to key data. When looking through its SGs we will only find  $SG_{KD}$  which should protect the *Confidentiality* of said data. There is also a direct connection from  $C_{1.1}$  to component  $C_1$  which is in a granularity level above.

According to the definition (Section 4.2.3) a sub-component can only process data that already exists in the abstraction layers above. Thus, a correct conclusion would be that if the confidentiality of key data is protected in  $C_{1.1}$  it is also protected in the layer above even though there is no explicit link between  $C_1$  and key data. This however, does *NOT* mean that the overall confidentiality is being protected since  $C_1$  may process other data, such as user data in the example.

Propagation from higher layers to lower ones is generally not possible without explicit links to data types. This will be discussed more thoroughly in Section 4.4.

Similar conclusions can be made for the *Integrity* of sub-components and its propagation to abstraction layers with higher or lower granularity levels with one slight difference. When looking at components at higher abstraction

layers we can say that if the integrity of a component  $C_1$  is being protected then all of its sub-components are being protected as well.

For *Availability* however, the situation differs. The connection between components (*hasComponent*) has been defined as a composition. This means that the availability of a specific sub-component is pre-determined by the structural features of the SUS. If the availability of a component  $C_1$  is protected it necessarily means that the availability of its sub-components is protected as well. To have the availability of a component protected however all of the sub-components have to be protected individually. The availability of a component is therefore the union of availabilities of its sub-components.

## Threats

Similar to SGs one can look into propagation rules for threats. Firstly we will look at the important attributes of a threat. The key attribute here will be *attackPotential* which will be considered during the transformation steps in Section 4.4.

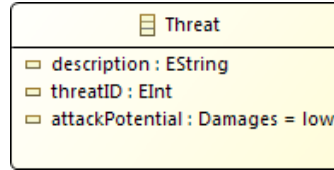


Figure 14: Attributes of a Threat

Here, the focus will be on the propagation of threats through granularity levels based on an underspecified security concept.

Every defined threat threatens at least one SG according to the metamodel (Figure 7) and since every SG addresses one asset (component or data) we can adapt the observations made in the previous section.





Figure 15: Underspecified Security Concept with a Threat

In Figure 15 a threat  $T_{SG_{UD}}$  threatens  $SG_{UD}$  which addresses the user data that is being used by sub-component  $C_{1.1}$ . The influence of  $T_{KD}$  on higher abstraction layers is of interest since neither SGs nor threats are explicitly defined in the example.

$SG_{UD}$  : The Confidentiality of sensible user data should be protected

$T_{SG_{UD}}$  : Eavesdropping on sensible user data

Similar to SGs, we can assume that  $T_{SG_{UD}}$  propagates to the layer above based on the definition of sub-components. User data, which is only explicitly addressed by  $SG_{UD}$ , is also present at parental nodes. Thus, if the *Confidentiality* of user data is being threatened by  $T_{SG_{UD}}$ , it is also being threatened when looking at  $C1$ .

For the propagation from abstraction layers depicting lower granularities ( $C_1$ ) to layers with higher granularity ( $C_{1.1}$ ) we have to take the data types into account. We will define a SG addressing key data and the corresponding threat.

$SG_{KD}$  : The Confidentiality of key data should be protected

$T_{SG_{KD}}$  : Disclosure of key data

Now if the the confidentiality is being threatened by  $T_{SG_{KD}}$  it is not clear how it will propagate to the layers below since  $C_{1.1}$  is not addressing key data in any observable way.

Threats that threaten SGs with *Integrity* as their security goal classes behave differently. Contrary to confidentiality, assumptions can be made when looking at propagation from higher abstraction layers to lower ones. When integrity of a component  $C_n$  is being threatened the integrity of all respective sub-components  $C_{n.1}...C_{n.m}$  is being threatened as well. If the integrity of a sub-component  $C_{n.i}$  is being threatened it will also propagate to its parental node  $C_n$  since a node can only be as secure as its sub-nodes.

Lastly, for *Availability* the propagation is pre-determined by the structural features and the definition of sub-components. If the availability of a component  $C_n$  is threatened it propagates to its sub-components  $C_{n.1}...C_{n.m}$ .

If the availability of one sub-component is being threatened it will also propagate to its parental nodes. This however does not provide information on how severely the availability of  $C_n$  as a whole will be impaired in case of an attack on the availability of  $C_{n.i}$ . This propagation from sub-components to their parental nodes is very similar to the just mentioned integrity behavior. The availability of  $C_n$  is a union of availabilities of its sub-components and one threat on a specific  $C_{n.i}$  would alter said set.

We can therefore conclude that to ensure a SG of a component  $C_n$  all its sub-components have to be protected as well. For threats however it is enough to threaten one sub-component to have an effect on its parental node.

## Controls

Controls try to mitigate threats and are directly linked to at least one threat at all times. The propagation of controls through abstraction layers will therefore be closely coupled with threats and SGs.



Figure 16: Underspecified Security Concept with a Control

We have already discussed the propagation of SGs and threats in the previous chapters and thus, indirectly the propagation of controls. The example in Figure 16 shows a control that mitigates the threat  $T_{SG_{UD}}$ . In natural text the security attributes could be the following:

$SG_{KD}$  : The Confidentiality of sensible user data should be protected

$T_{SG_{KD}}$  : Eavesdropping on sensible user data

$C_{T_{SG_{KD}}}$  : Encryption of sensible user data with AES-256 to prevent eavesdropping

Similar to threats which propagate to the upper abstraction layers, controls will as well. The rules will be the same since the controls are very tightly coupled and cannot exist without threats.

For this example this would mean that when looking at the abstraction layer above and at  $C_1$  we will consider the control  $C_{T_{SG_{KD}}}$  as well the threat  $T_{SG_{KD}}$  it is mitigating.

This section was only giving an overview on the conclusions for security attributes that can be made based on the structural features of an (under-specified) security concept definition. A more thorough definition will be discussed in the following section.

### 4.3 Model Transformation

Let  $SG_{CIA}(SUS)$  be the set of security goals for a SUS. A security goal SG is defined as  $SG(cl, c, asset, dmg)$  where  $cl$  is the security goal class ( $C$  for

confidentiality,  $I$  for Integrity and  $A$  for availability),  $c$  being the component,  $asset$  being the element of interest which the SG was defined for, i.e. the component itself or data which is being processed by it and  $dmg$  is the damage potential in case of a security breach ( $H$  = high,  $M$  = medium and  $L$  = low). Similarly we define a threat set  $T_{STRIDE}$  for a SUS where STRIDE is the threat modeling technique developed by Microsoft. According to [20] a component can be exposed to the following threats:

**Spoofing:** Adversaries pretend to be someone else

**Tampering:** Adversaries change data in transit

**Repudiation:** Adversaries perform actions that can't be traced back to them

**Information disclosure:** Unauthorized viewing/stealing of data

**Denial of service:** Interruption of system services

**Elevation of privilege:** Performing of unauthorized actions

Every threat has therefore a specific threat class that it can be assigned to.  $T_{STRIDE}$  is the set of threats where  $T(tc, sg, sev)$  is a threat,  $tc$  being the threat class,  $sg$  being the security goal which the threat violates and  $sev$  being the severity of the threat if successfully exploited ( $H$  = high,  $M$  = medium and  $L$  = low).

Controls are tightly coupled with security goals and threats.  $C_{SUS}$  is the set of controls for a SUS that contains all the controls. A Control  $C(T)$  has a set of threats  $T$  it mitigates.

Each asset can be viewed separately when looking at security goals and threats. For SGs we can define three separate sets,  $SG_C(c)$ ,  $SG_I(c)$  and  $SG_A(c)$  where each one contains the respective SGs with either confidentiality, integrity or availability as the security goal class.

**Definition 2**  $SG_{CIA}(c) = SG_C(c) \cup SG_I(c) \cup SG_A(c)$

The respective sets covering one security goal class can be defined as follows:

**Definition 3**  $SG_{sgc}(c) = SG(sgc, c, asset_j, dmg) \cup SG(sgc, c, asset_{j+1}, dmg) \cup \dots \cup SG(sgc, c, asset_m, dmg)$

Threats can be defined accordingly. For a threat  $T$  with the threat class  $tc$  the following union set can be defined.

**Definition 4**  $T_{tc}(c) = T(tc, sg_i, sev) \cup T(tc, sg_{i+1}, sev) \cup \dots \cup T(tc, sg_n, sev) | sg_i \in SG_{CIA}(c)$

The set  $T_{STRIDE}$  is therefore a union of all threat sets:

**Definition 5**  $T_{STRIDE}(c) = T_S(c) \cup T_T(c) \cup T_R(c) \cup T_I(c) \cup T_D(c) \cup T_E(c)$

The just mentioned sets are the basic sets for components without looking at structural features of a SUS. As mentioned in Section 2.2 we can derive further security properties from sub-components and overall structural features of the system. This derivation will be covered in the following Sections.

## 4.4 Transformation Rule Set for Security Goals

### 4.4.1 Aggregation Rules

## 4.5 Transformation Rule Set for Threats

### 4.5.1 Aggregation Rules

## 4.6 Transformation Rule Set for Controls

### 4.6.1 Aggregation Rules

# 5 Implementation

## 5.1 Technology

## 5.2 Validity & Verification

## 5.3 Runtime & Complexity

# 6 Summary

# 7 Outlook

## References

- [1] ISO/IEC 27001:2005 - information technology – security techniques – information security management systems – requirements. Technical report, 2005.
- [2] Mark Branagan, Robert Dawson, and Dennis Longley. Security risk analysis for complex systems. pages 1–12, 2006.
- [3] F. Fleurey, J. Steel, and B. Baudry. Validation in model-driven engineering: testing model transformations. In *Proceedings. 2004 First International Workshop on Model, Design and Validation, 2004.*, pages 29–40, Nov 2004.
- [4] Morrie Gasser. *Building a Secure Computer System*. Van Nostrand Reinhold Co., New York, NY, USA, 1988.
- [5] Frédéric Jouault, Freddy Allilaire, Jean Bézivin, and Ivan Kurtev. Atl: A model transformation tool. *Science of Computer Programming*, 72(1):31 – 39, 2008.
- [6] Prathaben Kanagasingham. Data loss prevention. *SANS Institute*. Aug, 2008.
- [7] Anneke G. Kleppe, Jos Warmer, and Wim Bast. *MDA Explained: The Model Driven Architecture: Practice and Promise*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2003.
- [8] Arjen Lenstra and Tim Voss. *Information Security Risk Assessment, Aggregation, and Mitigation*, pages 391–401. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.
- [9] Tom Mens and Pieter Van Gorp. A taxonomy of model transformation. *Electronic Notes in Theoretical Computer Science*, 152:125 – 142, 2006. Proceedings of the International Workshop on Graph and Model Transformation (GraMoT 2005).
- [10] 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.
- [11] J. M. Mottu, B. Baudry, and Y. L. Traon. Model transformation testing: oracle issue. In *2008 IEEE International Conference on Software Testing Verification and Validation Workshop*, pages 105–112, April 2008.

- [12] 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.
- [13] OMG. OMG Meta Object Facility (MOF) Core Specification, Version 2.4.1, June 2013.
- [14] Charles P. Pfleeger and Shari Lawrence Pfleeger. *Security in Computing (4th Edition)*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2006.
- [15] Klaus Pohl, Harald Hönniger, Reinhold Achatz, and Manfred Broy. *Model-Based Engineering of Embedded Systems: The SPES 2020 Methodology*. Springer Publishing Company, Incorporated, 2012.
- [16] Dorothy Elizabeth Robling Denning. *Cryptography and data security*. Addison-Wesley Longman Publishing Co., Inc., 1982.
- [17] E. Seidewitz. What models mean. *IEEE Software*, 20(5):26–32, Sept 2003.
- [18] The Common Criteria Recognition Agreement Members. Common criteria for information technology security evaluation. <http://www.commoncriteriaportal.org/>, September 2012.
- [19] 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.
- [20] P. Torr. Demystifying the threat modeling process. *IEEE Security Privacy*, 3(5):66–70, Sept 2005.
- [21] J.R. Vacca. *Computer and Information Security Handbook*. Elsevier Science, 2012.