Security Requirements Document

Netflix Security Requirements

Omer Irfan

Feb 12, 2021

This document has been generated by STS-Tool

http://www.sts-tool.eu

Table of Contents:

Introduction

This document describes the security requirements for the "Netflix Security Requirements"project. It provides a detailed description of: (I)social and organizational model, while capturing security requirements and automated analysis results;

Social and organizational models

This section provides a detailed description of the socio-technical security requirements models from different views (*Social*, *Information*, *Authorization*) and then presents the list of *security requirements* derived from them.

The *Social view* represents stakeholders as intentional and social entities, representing their goals and important information in terms of documents, together with their interactions with other actors to achieve these goals and to exchange information. Stakeholders express constraints over their interactions in terms of *security needs.* The *Information view* represents the informational content of stakeholders' documents, showing how information and documents are interconnected, as well as how they are composed respectively. The *Authorization view* represents which stakeholders own what information, and captures the flow of permissions or prohibitions from one stakeholder to another. The modelling of authorizations expresses other *security needs* related to the way information is to be manipulated.

The section ends with the list of *security requirements* for the system to be expressed in terms of *social commitments*, namely promises with contractual validity stakeholders make to one another. The security requirements are derived automatically once the modelling is done and the designer has captured the security needs expressed by stakeholders. Whenever a security need is expressed over an interaction from one stakeholder to the other, a commitment on the opposite direction is expected from the second stakeholder to satisfy the security need.

Social View

The social view shows the involved stakeholders, which are represented as *roles* and *agents*. Agents refer to actual participants (stakeholders) known when modelling the Netflix Security Requirements project, whereas roles are a generalisation (abstraction) of agents. To capture the connection between roles and agents, the *play* relation is used to express the fact that certain agents play certain roles.

Stakeholders have goals to achieve and they make use of different information to achieve these goals. They interact with one another mainly by *delegating goals* and *exchanging information*. Information is represented by means of documents, which actors manipulate to achieve their goals.

Social View Diagram

Figure 1 presents the graphical representation of the social view (a larger picture is shown in appendix A).

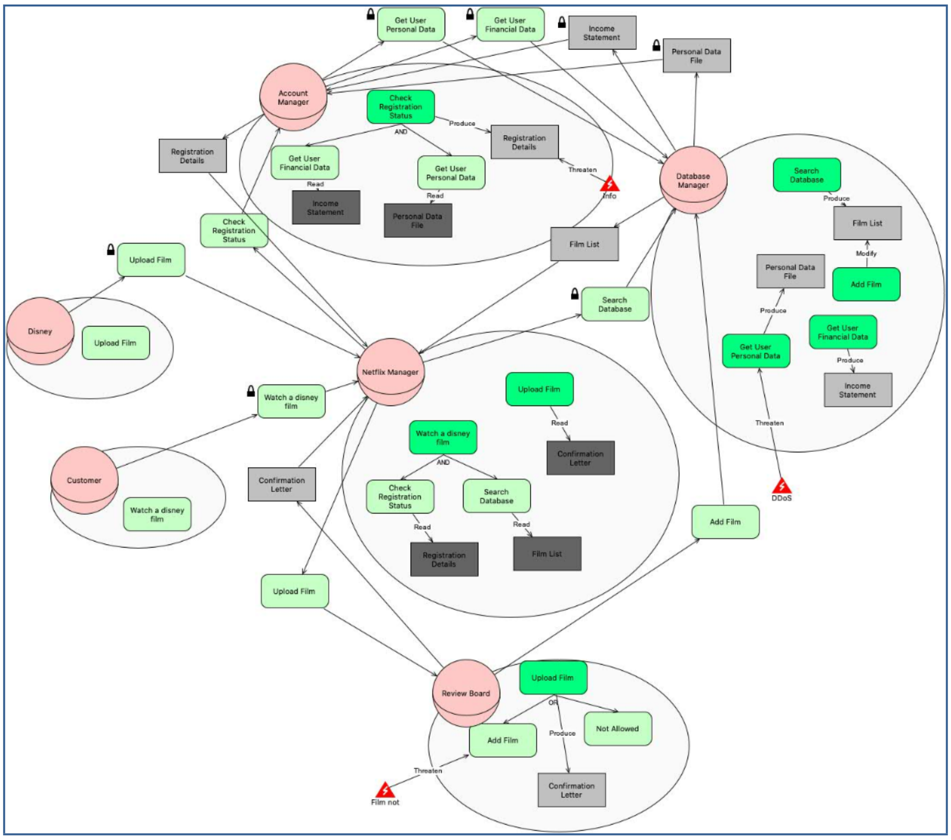

Figure 1 - Social View for the Netflix Security Requirements project

Stakeholders

This section describes the stakeholders identified in the Netflix Security Requirements project. Stakeholders are represented as roles or agents.

In particular, identified roles are: *Customer*, *Netflix Manager*, *Database Manager*, *Account Manager*, *Disney* and *Review Board* (Figure 1). Table 1 summarise the stakeholders.

Role	Description	Mission	Purpose
Customer	An End-User for Netflix		Prupose is to watch a disney film.
Netflix Manager	Manager of Netflix Branch		Handles main operations required by Netflix App
Database Manager	Stores all data of users and films		Modifys film catalogue and distributed user data to required personnel
Account Manager	A system to register users		Organizes users' registration details in one place.
Disney	Disney Studios		Provides films for Netflix to upload on thier syste for users.
Review Board	This board review films fron different studios for adding them to Netflix		There purpose is to apporve or disprove films for Netflix

Table 1 - Roles in the Netflix Security Requirements project.

In the Netflix Security Requirements project there are no plays relationships taking place for the given agents/roles.

Stakeholders' documents

Stakeholders have documents they possess or exchange with others to achieve their goals. Documents are represented within the rationale of the role/agent (Figure 1).

In the Netflix Security Requirements project (Figure 1) we have:

☐ **Netflix Manager** has document *Registration Details* provided by *Account Manager*, document *Confirmation Letter* provided by *Review Board* and document *Film List* provided by *Database Manager*.

☐ **Database Manager** has documents *Film List*, *Personal Data File* and *Income Statement*.

☐ **Account Manager** has document *Registration Details*. Moreover it has document *Personal Data File* provided by *Database Manager* and document *Income Statement* provided by *Database Manager*.

☐ **Review Board** has document *Confirmation Letter*.

Table 2 summarises stakeholders' *documents* for the Netflix Security Requirements project.

Agent/Role	Document	Description
Netflix Manager	Confirmation Letter	
	Film List	
	Registration Details	
Database Manager	Film List	
	Personal Data File	
	Income Statement	
Account Manager	Income Statement	
	Personal Data File	
	Registration Details	
Review Board	Confirmation Letter	

Table 2 - Stakeholders' documents in the Netflix Security Requirements project

Stakeholders' documents and goals

Stakeholders' documents are linked to their goals: they read (make) documents to achieve their goals, they modify documents while achieving their goals, and they may produce documents from achieving their goals.

In the Netflix Security Requirements project (Figure 1) stakeholders' documents and goals are related as follows:

□ **Netflix Manager** *reads* document *Film List* to achieve goal *Search Database*, *reads* document *Confirmation Letter* to achieve goal *Upload Film* and *reads* document *Registration Details* to achieve goal *Check Registration Status*.

□ **Database Manager** *produces* document *Personal Data File* to achieve goal *Get User Personal Data*, *produces* document *Income Statement* to achieve goal *Get User Financial Data*, *produces* document *Film List* to achieve goal *Search Database* and *modifies* document *Film List* to achieve goal *Add Film*.

□ **Account Manager** *reads* document *Income Statement* to achieve goal *Get User Financial Data*, *produces* document *Registration Details* to achieve goal *Check Registration Status* and *reads* document *Personal Data File* to achieve goal *Get User Personal Data*.

□ **Review Board** *produces* document *Confirmation Letter* to achieve goal *Upload Film*.

Table 3 summarises goal-document relations for all stakeholders in the Netflix Security Requirements project.

Agent/Role	Goal	Document	Relation
Netflix Manager	Search Database	Film List	Read
	Upload Film	Confirmation Letter	Read
	Check Registration Status	Registration Details	Read
Database Manager	Get User Personal Data	Personal Data File	Produce
	Get User Financial Data	Income Statement	Produce
	Search Database	Film List	Produce
	Add Film	Film List	Modify

Account Manager	Get User Financial Data	Income Statement	Read
	Check Registration Status	Registration Details	Produce
	Get User Personal Data	Personal Data File	Read
Review Board	Upload Film	Confirmation Letter	Produce

Table 3 - Relation of stakeholders' documents to their goals

Goal Refinement

Stakeholders have goals to achieve. Goals are represented within the rationale (round compartment attached to the role/agent, see Figure 1) of the role/agent representing the stakeholder. They achieve their goals by further refining them into finer-grained goals (subgoals) by means of AND/OR-decompositions. AND-decompositions structurally refine a goal into multiple subgoals (all AND subgoals need to be achieved for the goal to be achieved), while OR-decompositions represent alternative ways for achieving a goal (at least one of the subgoals in the OR-decomposition needs to be achieved for the goal to be achieved).

In the Netflix Security Requirements project (Figure 1) we have:

□ **Customer** has to achieve goal *Watch a disney film*.

□ **Netflix Manager** has to achieve goal *Watch a disney film* and goal *Upload Film*. To achieve *Watch a disney film*, Netflix Manager should achieve goal *Search Database* and goal *Check Registration Status*

□ **Database Manager** has to achieve goal *Search Database*, goal *Add Film*, goal *Get User Personal Data* and goal *Get User Financial Data*.

□ **Account Manager** has to achieve goal *Check Registration Status*. To achieve *Check Registration Status*, Account Manager should achieve goal *Get User Financial Data* and goal *Get User Personal Data*

□ **Disney** has to achieve goal *Upload Film*.

□ **Review Board** has to achieve goal *Upload Film*. To achieve *Upload Film*, Review Board should achieve either goal *Not Allowed* or goal *Add Film*

Table 4 summarises the goals of each agent/role in the Netflix Security Requirements project and how they are decomposed, when applicable.

Agent/Role	Goal	Dec. Type	Subgoals
Customer	Watch a disney film	-	
Netflix Manager	Watch a disney film	AND	Search Database Check Registration Status
	Upload Film	-	
Database Manager	Search Database	-	
	Add Film	-	
	Get User Personal Data	-	
	Get User Financial Data	-	
Account Manager	Check Registration Status	AND	Get User Financial Data Get User Personal Data
Disney	Upload Film	-	
Review Board	Upload Film	OR	Not Allowed Add Film

Table 4 - Goal Decompositions

Goal Contributions

Goals can contribute one to another. A contribution identifies the impact the fulfilment of one goal has on the fulfilment of another goal. This impact can be either positive or negative, and is represented with "++" and "--" respectively. Positive contribution means that the achievement of a goal also achieves the other goal. Negative contribution means that the achievement of a goal inhibits the achievement of another goal.

In the Netflix Security Requirements project there are no contribution relations taking place for the given agents/roles.

Stakeholders Interactions

This section describes stakeholders' interactions, providing insights on whom they interact with to fulfil their desired objectives, as well as which are the stakeholders that rely on them to fulfil their respective goals. This kind of interaction is carried out by means of *goal delegations*.

To achieve their goals stakeholders might need specific information. If they do not possess this information, they may ask other stakeholders to provide them documents. *Document transmission* is used to capture this interaction.

Goal Delegations

Stakeholders interact with others to achieve some of their goals by means of goal delegations. Goal delegations are graphically represented as a relation that starts from a delegator actor to a delegatee actor (following the direction of the arrow), having a rounded corner rectangle representing the goal being delegated. Security needs are graphically specified as labels that appear below the delegated goal (Figure 1).

The following description enlists all the delegations from one role/agent to the others. When applicable, security needs expressed over the delegations are enumerated.

In the Netflix Security Requirements project (Figure 1), we have the following goal delegations:

☐ **Customer** delegates goal *Watch a disney film* to **Netflix Manager**.

The following security needs apply to this delegation:

Non Repudiation: acceptance.

☐ **Netflix Manager** delegates goal *Check Registration Status* to **Account Manager**.

☐ **Netflix Manager** delegates goal *Search Database* to **Database Manager**.

The following security needs apply to this delegation:

Non Repudiation: acceptance.

☐ **Netflix Manager** delegates goal *Upload Film* to **Review Board**.

☐ **Account Manager** delegates goal *Get User Personal Data* to **Database Manager**.

The following security needs apply to this delegation:

Trustworthiness.

□ **Account Manager** delegates goal *Get User Financial Data* to **Database Manager**.

The following security needs apply to this delegation:

Trustworthiness.

□ **Disney** delegates goal *Upload Film* to **Netflix Manager**.

The following security needs apply to this delegation:

Trustworthiness.

□ **Review Board** delegates goal *Add Film* to **Database Manager**.

Table 5 summarises *goal delegations*, together with the eventual *security needs* when applicable, and eventual description respectively.

Delegator	Goal	Delegatee	Security Needs	Delegation Description
Customer	Watch a disney film	Netflix Manager	**Non Repudiation**: *acceptance*	
Netflix Manager	Check Registration Status	Account Manager		
	Search Database	Database Manager	**Non Repudiation**: *acceptance*	
	Upload Film	Review Board		
Account Manager	Get User Personal Data	Database Manager	**Trustworthiness**	
	Get User Financial Data	Database Manager	**Trustworthiness**	
Disney	Upload Film	Netflix Manager	**Trustworthiness**	
Review Board	Add Film	Database Manager		

Table 5 - Goal Delegations and Security Needs

Document Transmission

Stakeholders exchange information by means of documents with other stakeholders. The following description enlists all the transmission from one role/agent representing the stakeholder, to other roles/agents. *Document transmission* is represented as an arrow from the transmitter to the receiver, with a rectangle representing the document. The security needs expressed over the transmission are described, if applicable. Security needs are specified with the help of labels that appear below the document being transmitted.

In the Netflix Security Requirements project (Figure 1), we have the following *document transmissions*:

□ **Database Manager** transmit document *Film List* to **Netflix Manager**.

□ **Database Manager** transmit document *Income Statement* to **Account Manager**.

The following security needs apply to this transmission:

Confidentiality: receiver.

□ **Database Manager** transmit document *Personal Data File* to **Account Manager**.

The following security needs apply to this transmission:

Confidentiality: receiver.

□ **Account Manager** transmit document *Registration Details* to **Netflix Manager**.

□ **Review Board** transmit document *Confirmation Letter* to **Netflix Manager**.

Table 6 summarises the *document transmissions* for the Netflix Security Requirements project.

Transmitter	Document	Receiver	Security Needs	Transmission Descr.
Database Manager	Film List	Netflix Manager		
	Income Statement	Account Manager	**Confidentiality**: *receiver*	
	Personal Data File	Account Manager	**Confidentiality**: *receiver*	
Account Manager	Registration Details	Netflix Manager		

Review Board	Confirmation Letter	Netflix Manager

Table 6 - Document Transmissions and Security Needs

Organisational Constraints

Apart from the security needs actors specify over their interactions, there are others, which are dictated either by the organisation, business rules and regulations, or law. In this section we enlist these constraints, together with the security requirements derived from them. Currently, the language supports these organisational constraints: *Separation of Duties (SoD)* and *Binding of Duties (BoD)*. Graphically we represent these constraints using a similar notation to that used in workflows, as a circle with the *unequal* sign within and as a circle with the *equals* sign within, respectively. The relations are symmetric, and as such they do not have any arrows pointed to the concepts they relate (being these roles or goals).

In the Netflix Security Requirements project there are no organisational constraints specified.

Events

Table 7 represents all the events modeled in the project Netflix Security Requirements together with the set of elements each event threatens. Additionally, for each reported event a textual description is provided.

Event name	Threatened elements	Description
DDoS Attack	GoalReference: Get User Personal Data	
Film not approved	Goal: Add Film	
Info Integrity Issue	Document: Registration Details	

Table 7 - Events

Information View

The information view gives a structured representation of the information and documents in the Netflix Security Requirements project. It shows what is the informational content of the documents represented in the social view. Information is represented by one or more documents (*tangible by*), and the same document can make tangible multiple information entities. Moreover, the information view considers composite documents (information) capturing these by means of *part of* relations.

Information View Diagram

Figure 2 presents the graphical representation of the information view.

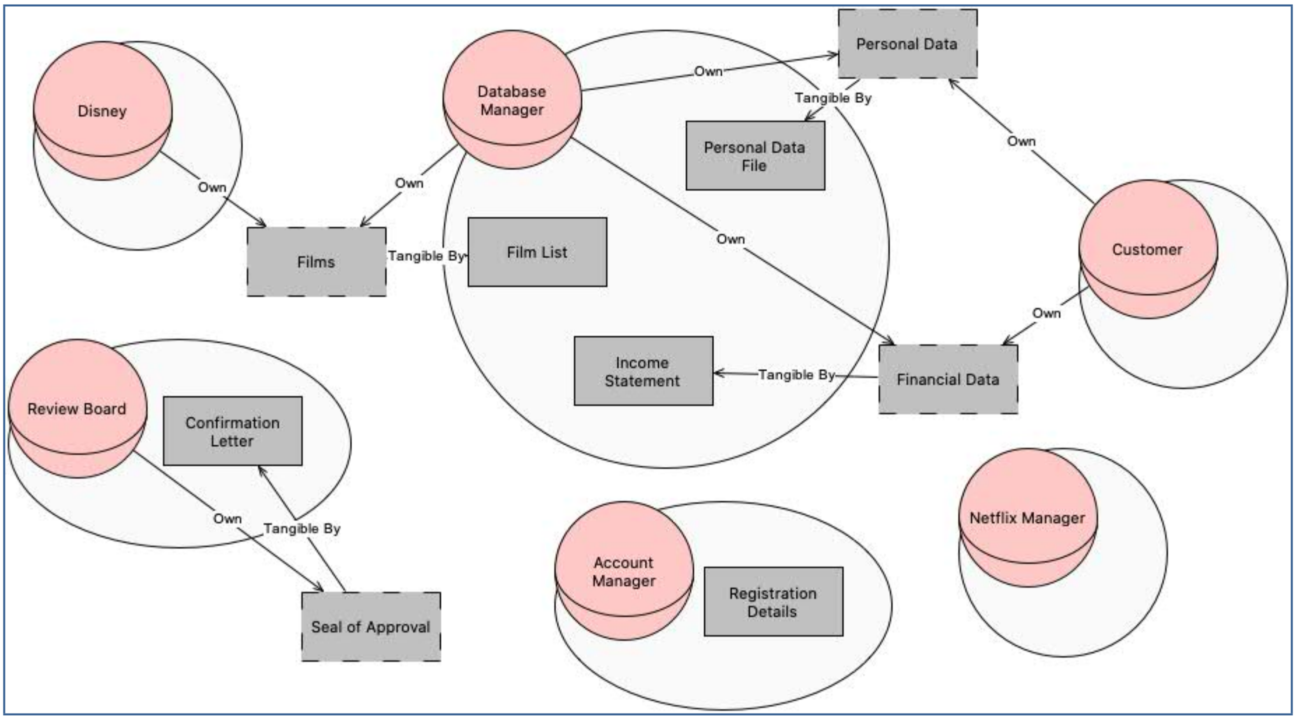

Figure 2 - Information View for the Netflix Security Requirements project

Modelling Ownership

The information view represents also who are the *owners* of the information that is being manipulated through the documents that represent them in the social view.

The owners for the different information in the Netflix Security Requirements project are summarised in Table 8.

Agent/Role	Information	Description
Customer	Personal Data	
	Financial Data	
Database Manager	Financial Data	
	Personal Data	
	Films	
Disney	Films	
Review Board	Seal of Approval	

Table 8 - Information owners

Representation of Information

Information is represented (*made tangible by*) by documents, which stakeholders have and exchange.

The documents stakeholders in the Netflix Security Requirements project (Figure 2) have and exchange with one another contain the information as summarised in Table 9:

Information	Document	Description
Financial Data	Income Statement	
Films	Film List	
Seal of Approval	Confirmation Letter	
Personal Data	Personal Data File	

Table 9 - Representation of Information through Documents

Structure of Information and Documents

Documents (information) are composed of other documents (information). Composition of documents (information) is captured through *part of* relations. This gives us an idea of how information and/or documents in the Netflix Security Requirements project are structured.

In the Netflix Security Requirements project there are no composite documents or information.

Authorization View

The authorization view shows the permissions or prohibitions flow from a stakeholder to another, that is, the authorizations stakeholders grant or deny to others about information, specifying the operations the others can and must perform over the information. Apart from granting authority on performing operations, a higher authority can be granted, that of further authorising other actors (i.e. authorization transferability)

Authorizations start from the information owner. Therefore, in the authorization view, ownership is preserved and inherited from the information view.

Authorization View Diagram

Figure 3 presents the graphical representation of the Authorization view (a larger picture is rappresented in appendix A).

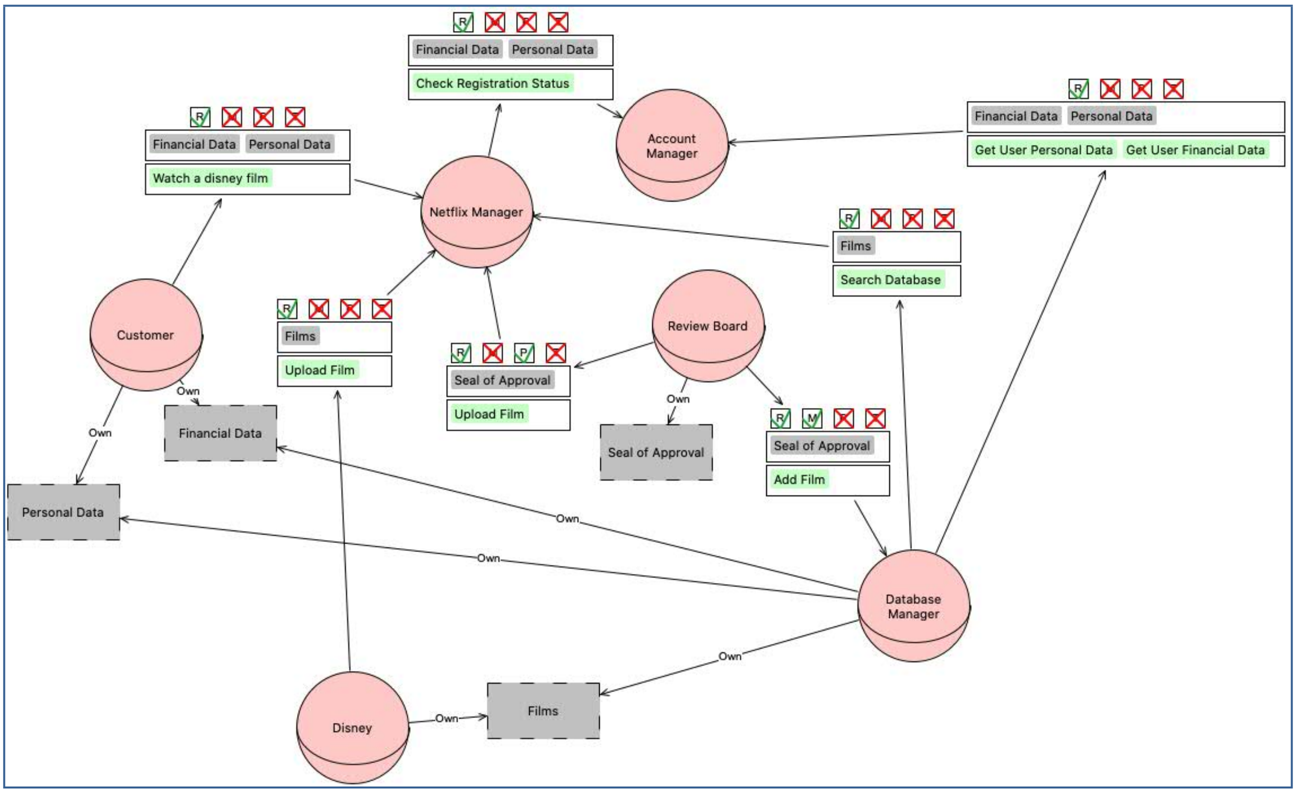

Figure 3 - Authorization View for the Netflix Security Requirements project

Authorization Flow

In this section are described for each role/agent, the authorizations it passes to others and what authorizations it receives from other roles/agents.In the Netflix Security Requirements project (Figure 3) the authorizations for each role/agent are:

- □ *Role* **Customer**:
  - **Customer** authorises *Netflix Manager* to *read* and prohibits to *modify*, *produce* and *transmit* information *Financial Data* and *Personal Data*, in the scope of goal *Watch a disney film*, *passing* the right to further authorising other actors.
- □ *Role* **Netflix Manager**:
  - **Netflix Manager** authorises *Account Manager* to *read* and prohibits to *modify*, *produce* and *transmit* information *Financial Data* and *Personal Data*, in the scope of goal *Check Registration Status*, *passing* the right to further authorising other actors.
  - **Netflix Manager** is authorised by *Netflix Manager* to *read* and prohibited to *modify*, *produce* and *transmit* information *Financial Data* and *Personal Data*, in the scope of goal *Watch a disney film*, *having* the right to further authorising other actors, and is authorised by *Netflix Manager* to *read* and prohibited to *modify*, *produce* and *transmit* information *Films*, in the scope of goal *Upload Film*, *having* the right to further authorising other actors, and is authorised by *Netflix Manager* to *read* and *produce* and prohibited to *modify* and *transmit* information *Seal of Approval*, in the scope of goal *Upload Film*, *having* the right to further authorising other actors, and is authorised by *Netflix Manager* to *read* and prohibited to *modify*, *produce* and *transmit* information *Films*, in the scope of goal *Search Database*, *having* the right to further authorising other actors.
- □ *Role* **Database Manager**:
  - **Database Manager** authorises *Account Manager* to *read* and prohibits to *modify*, *produce* and *transmit* information *Financial Data* and *Personal Data*, in the scope of goals *Get User Personal Data* and *Get User Financial Data*, *passing* the right to further authorising other actors, and authorises *Netflix Manager* to *read* and prohibits to *modify*, *produce* and *transmit* information *Films*, in the scope of goal *Search Database*, *passing* the right to further authorising other actors.

- **Database Manager** is authorised by *Database Manager* to *read* and *modify* and prohibited to *produce* and *transmit* information *Seal of Approval*, in the scope of goal *Add Film*, *having* the right to further authorising other actors.

□ *Role* **Account Manager**:

- **Account Manager** s.
- **Account Manager** is authorised by *Account Manager* to *read* and prohibited to *modify*, *produce* and *transmit* information *Financial Data* and *Personal Data*, in the scope of goal *Check Registration Status*, *having* the right to further authorising other actors, and is authorised by *Account Manager* to *read* and prohibited to *modify*, *produce* and *transmit* information *Financial Data* and *Personal Data*, in the scope of goal *Get User Personal Data* and *Get User Financial Data*, *having* the right to further authorising other actors.

□ *Role* **Disney**:

- **Disney** authorises *Netflix Manager* to *read* and prohibits to *modify*, *produce* and *transmit* information *Films*, in the scope of goal *Upload Film*, *passing* the right to further authorising other actors.

□ *Role* **Review Board**:

- **Review Board** authorises *Database Manager* to *read* and *modify* and prohibits to *produce* and *transmit* information *Seal of Approval*, in the scope of goal *Add Film*, *passing* the right to further authorising other actors, and authorises *Netflix Manager* to *read* and *produce* and prohibits to *modify* and *transmit* information *Seal of Approval*, in the scope of goal *Upload Film*, *passing* the right to further authorising other actors.

Security Requirements

This section provides the list of security requirements derived for the Netflix Security Requirements project.

The list of security requirements shows the roles/agents that are *responsible* to satisfy them, so that stakeholders know what they have to bring about in order to satisfy the corresponding security needs. Security requirements also include the authorizations granted by stakeholders to other stakeholders.

Security needs are expressed mainly over goal delegations, document provisions and authorizations. Therefore, the list of security requirements is derived from every type of security need. Moreover, the organisational constraints specify further *needs* over roles and goal, leading to the generation of other security requirements.

Finally, the *requester* actors are represented to capture the actors requiring certain security needs to be brought about.

The security requirements for the Netflix Security Requirements project (Table 10) are:

□ **Customer** requires *Netflix Manager non-repudiation-of-acceptance* of the delegation of goal *Watch a disney film*, when delegating *Watch a disney film* to *Netflix Manager*.

□ **Customer** requires *Netflix Manager* the *non-modification*, *non-production* and *non-disclosure* of information *Financial Data* and *Personal Data*, and *need-to-know* of these pieces of informations for the goal *Watch a disney film*, when authorising *Netflix Manager* to *read Financial Data* and *Personal Data* in the scope of goal *Watch a disney film*.

□ **Netflix Manager** requires *Database Manager non-repudiation-of-acceptance* of the delegation of goal *Search Database*, when delegating *Search Database* to *Database Manager*.

□ **Netflix Manager** requires *Account Manager* the *non-modification*, *non-production* and *non-disclosure* of information *Financial Data* and *Personal Data*, and *need-to-know* of these pieces of informations for the goal *Check Registration Status*, when authorising *Account Manager* to *read Financial Data* and *Personal Data* in the scope of goal *Check Registration Status*.

□ **Database Manager** requires *Account Manager* a *receiver-confidentiality* , when transmitting *Income Statement* to *Account Manager*requires *Account Manager* a *receiver-confidentiality* , when transmitting *Personal Data File* to *Account Manager*.

□ **Database Manager** requires *Account Manager* the *non-modification*, *non-production* and *non-disclosure* of information *Financial Data* and *Personal Data*, and *need-to-know* of these pieces of informations for the goals *Get User Personal Data* and *Get User Financial Data*, when authorising *Account Manager* to *read Financial Data* and *Personal Data* in the scope of goals *Get User Personal Data* and *Get User Financial Data*; while it requires *Netflix Manager* the *non-modification*, *non-production* and *non-disclosure* of information *Films*, and *need-to-know* of these pieces of information for the goal *Search Database*, when authorising *Netflix Manager* to *read Films* in the scope of goal *Search Database*.

□ **Account Manager** requires *Database Manager trustworthiness*, when delegating *Get User Personal Data* to *Database Manager*, while it requires *Database Manager trustworthiness*, when delegating *Get User Financial Data* to *Database Manager*.

□ **Disney** requires *Netflix Manager trustworthiness*, when delegating *Upload Film* to *Netflix Manager*.

□ **Disney** requires *Netflix Manager* the *non-modification*, *non-production* and *non-disclosure* of information *Films*, and *need-to-know* of these pieces of information for the goal *Upload Film*, when authorising *Netflix Manager* to *read Films* in the scope of goal *Upload Film*.

□ **Review Board** requires *Database Manager* the *non-production* and *non-disclosure* of information *Seal of Approval*, and *need-to-know* of these pieces of information for the goal *Add Film*, when authorising *Database Manager* to *read* and *modify Seal of Approval* in the scope of goal *Add Film*; while it requires *Netflix Manager* the *non-modification* and *non-disclosure* of information *Seal of Approval*, and *need-to-know* of these pieces of information for the goal *Upload Film*, when authorising *Netflix Manager* to *read* and *produce Seal of Approval* in the scope of goal *Upload Film*.

Responsible	Security Requirement	Requester	Description
Netflix Manager	non-repudiation-of-	Customer	Customer require non-

acceptance (delegated(Customer,Netflix Manager,Watch a disney film))		repudiation-of-acceptance for goal Watch a disney film,when delegating Watch a disney film to Netflix Manager.
non-modification (Financial Data,Personal Data)	Customer	Customer requires Netflix Manager non-modification of Information Financial Data and Personal Data.
non-production (Financial Data,Personal Data)	Customer	Customer requires Netflix Manager non-production of Information Financial Data and Personal Data.
non-disclosure (Financial Data,Personal Data)	Customer	Customer requires Netflix Manager non-disclosure of Information Financial Data and Personal Data.
need-to-know (Financial Data,Personal Data) (Watch a disney film)	Customer	Customer requires Netflix Manager need-to-know of Information Financial Data and Personal Data, in the scope of goal Watch a disney film.
non-modification (Films)	Disney	Disney requires Netflix Manager non-modification of Information Films.
non-production (Films)	Disney	Disney requires Netflix Manager non-production of Information Films.
non-disclosure (Films)	Disney	Disney requires Netflix Manager non-disclosure of Information Films.
need-to-know (Films) (Upload Film)	Disney	Disney requires Netflix Manager need-to-know of Information Films, in the scope of goal Upload Film.
non-modification (Seal of Approval)	Review Board	Review Board requires Netflix Manager non-modification of Information Seal of Approval.

	non-disclosure (Seal of Approval)	Review Board	Review Board requires Netflix Manager non-disclosure of Information Seal of Approval.
	need-to-know (Seal of Approval) (Upload Film)	Review Board	Review Board requires Netflix Manager need-to-know of Information Seal of Approval, in the scope of goal Upload Film.
	non-modification (Films)	Database Manager	Database Manager requires Netflix Manager non-modification of Information Films.
	non-production (Films)	Database Manager	Database Manager requires Netflix Manager non-production of Information Films.
	non-disclosure (Films)	Database Manager	Database Manager requires Netflix Manager non-disclosure of Information Films.
	need-to-know (Films) (Search Database)	Database Manager	Database Manager requires Netflix Manager need-to-know of Information Films, in the scope of goal Search Database.
Database Manager	non-repudiation-of-acceptance (delegated(Netflix Manager,Database Manager,Search Database))	Netflix Manager	Netflix Manager require non-repudiation-of-acceptance for goal Search Database,when delegating Search Database to Database Manager.
	non-production (Seal of Approval)	Review Board	Review Board requires Database Manager non-production of Information Seal of Approval.
	non-disclosure (Seal of Approval)	Review Board	Review Board requires Database Manager non-disclosure of Information

			Seal of Approval.
	need-to-know (Seal of Approval) (Add Film)	Review Board	Review Board requires Database Manager need-to-know of Information Seal of Approval, in the scope of goal Add Film.
Account Manager	trustworthiness (Database Manager, delegated(Account Manager,Database Manager,Get User Personal Data))	Account Manager	Database Manager shall provide proof of trustworthiness for Account Manager to delegate him goal Get User Personal Data.
	trustworthiness (Database Manager, delegated(Account Manager,Database Manager,Get User Financial Data))	Account Manager	Database Manager shall provide proof of trustworthiness for Account Manager to delegate him goal Get User Financial Data.
	recivier-confidentiality (transmitted(Database Manager,Account Manager,Income Statement))	Database Manager	Account Manager shall ensure the confidentiality of transmission of the document Income Statement being transmitted.
	recivier-confidentiality (transmitted(Database Manager,Account Manager,Personal Data File))	Database Manager	Account Manager shall ensure the confidentiality of transmission of the document Personal Data File being transmitted.
	non-modification (Financial Data,Personal Data)	Netflix Manager	Netflix Manager requires Account Manager non-modification of Information Financial Data and Personal Data.
	non-production (Financial Data,Personal Data)	Netflix Manager	Netflix Manager requires Account Manager non-production of Information Financial Data and Personal Data.

	non-disclosure (Financial Data,Personal Data)	Netflix Manager	Netflix Manager requires Account Manager non-disclosure of Information Financial Data and Personal Data.
	need-to-know (Financial Data,Personal Data) (Check Registration Status)	Netflix Manager	Netflix Manager requires Account Manager need-to-know of Information Financial Data and Personal Data, in the scope of goal Check Registration Status.
	non-modification (Financial Data,Personal Data)	Database Manager	Database Manager requires Account Manager non-modification of Information Financial Data and Personal Data.
	non-production (Financial Data,Personal Data)	Database Manager	Database Manager requires Account Manager non-production of Information Financial Data and Personal Data.
	non-disclosure (Financial Data,Personal Data)	Database Manager	Database Manager requires Account Manager non-disclosure of Information Financial Data and Personal Data.
	need-to-know (Financial Data,Personal Data) (Get User Personal Data,Get User Financial Data)	Database Manager	Database Manager requires Account Manager need-to-know of Information Financial Data and Personal Data, in the scope of goal Get User Personal Data and Get User Financial Data.
Disney	trustworthiness (Netflix Manager, delegated(Disney,Netflix Manager,Upload Film))	Disney	Netflix Manager shall provide proof of trustworthiness for Disney to delegate him goal Upload Film.

Table 10 - Security Requirements for the Netflix Security Requirements Project

Table 11 summarises the authorizations actors in the Netflix Security Requirements project grant to one another.

Authorisor	Information	Goal	Allowed Operations	Denied Operations	Authorisee	Description
Customer	Financial Data Personal Data	Watch a disney film	R	M, P, T	Netflix Manager	Transferable authority
Netflix Manager	Financial Data Personal Data	Check Registration Status	R	M, P, T	Account Manager	Transferable authority
Database Manager	Financial Data Personal Data	Get User Personal Data Get User Financial Data	R	M, P, T	Account Manager	Transferable authority
	Films	Search Database	R	M, P, T	Netflix Manager	Transferable authority
Disney	Films	Upload Film	R	M, P, T	Netflix Manager	Transferable authority
Review Board	Seal of Approval	Add Film	R, M	P, T	Database Manager	Transferable authority
	Seal of Approval	Upload Film	R, P	M, T	Netflix Manager	Transferable authority

Table 11 - Authorizations in the Netflix Security Requirements project

Well-formedness Analysis

The purpose of well-formedness analysis is to verify whether the diagram for the project Netflix Security Requirements is consistent and valid. A diagram is considered to be consistent if its constituent elements (concepts and relationships) are drawn and interconnected following the semantics of the modelling language (STS-ml in our case). Thus, well-formedness analysis performs post checks to verify compliance with STS-ml semantics for all checks that cannot be performed live over the models.

More details about the performed checks and their purpose can be found in Appendix B.

The Well-formedness Analysis analysis for Netflix Security Requirements project didn't find any errors.

Security Analysis

The purpose of security analysis is to verify whether the diagram for the project Netflix Security Requirements allows the satisfaction of the specified security needs or not. As a result, for all security needs expressed by stakeholders, it checks in the model whether there is any possibility for the security need to be violated. This analysis takes into account the semantics of STS-ml, defining the behaviour of the different elements represented in the models. The elements' behaviour is defined by propagation rules that consider what concepts and what relationships the specification of a given security need affects. Datalog is used to define the semantics of STS-ml to express facts (things always hold) and rules.

You can find more details about the performed checks in Appendix C.

The Security Analysis analysis for Netflix Security Requirements project didn't find any errors.

Appendix A

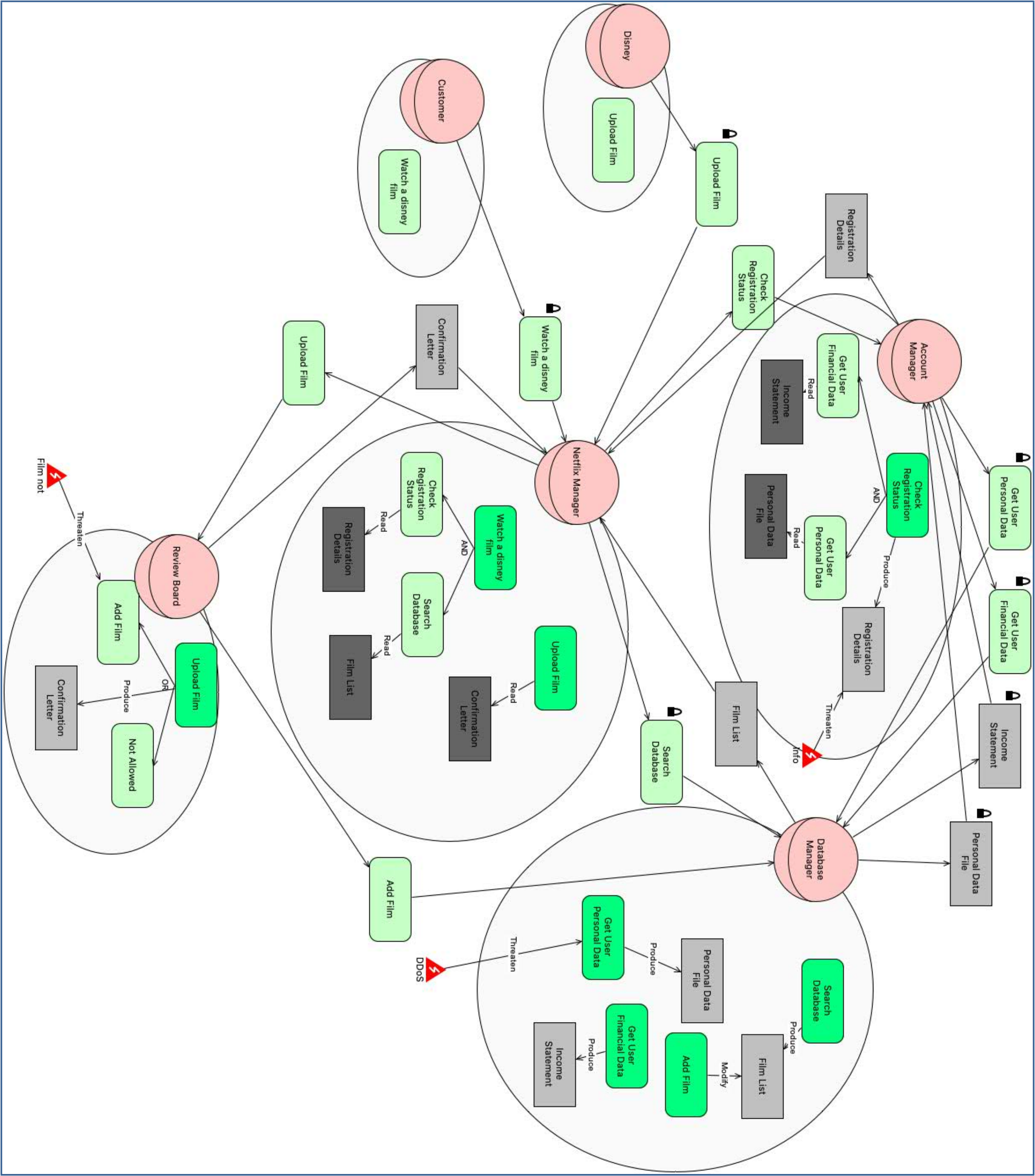

Figure 1 - Social View for the Netflix Security Requirements project

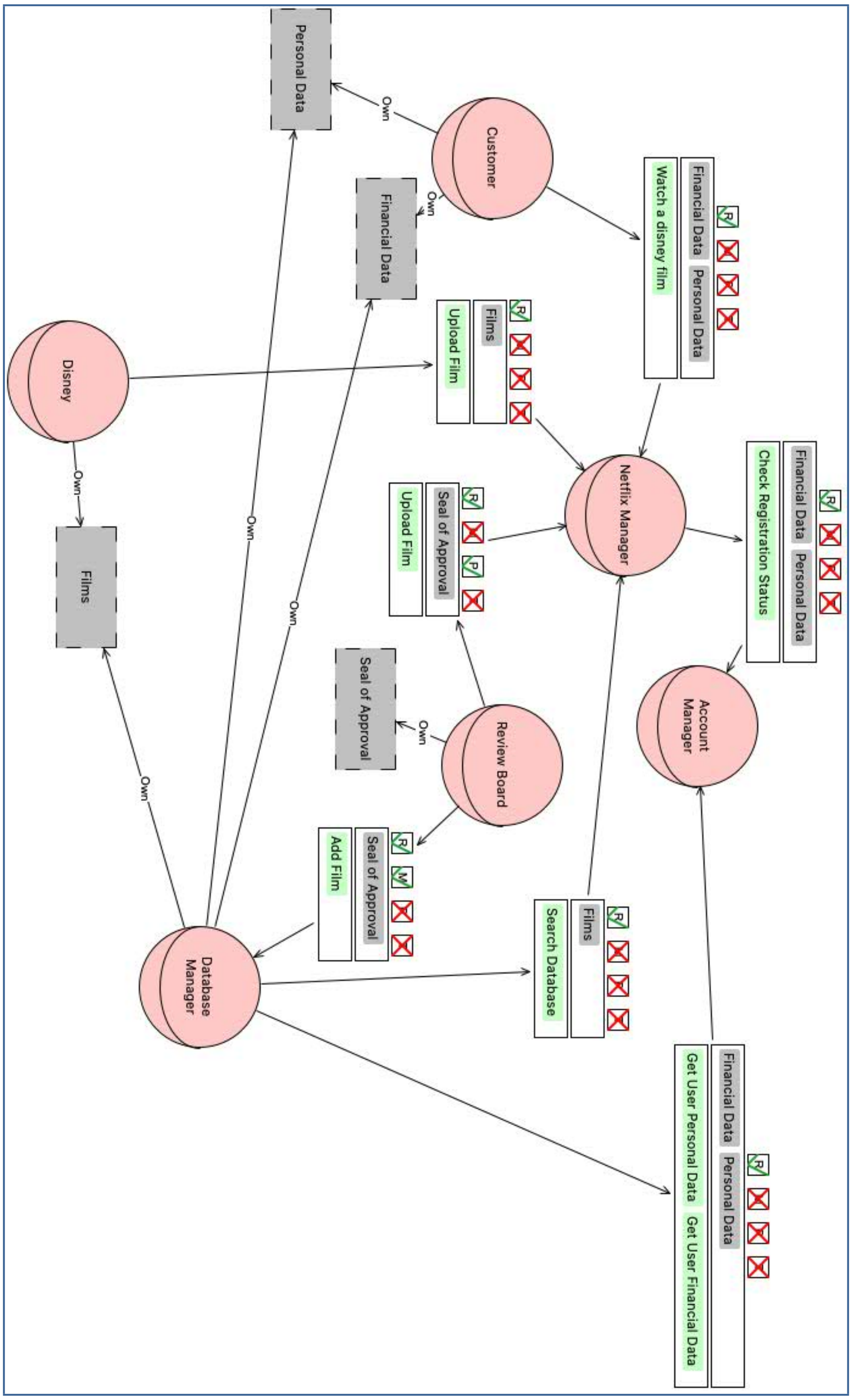

Figure 3 - Authorization View for the Netflix Security Requirements project

Appendix B

Details of Well-formedness analysis:

□ **Empty Diagram**

This check verifies whether the given diagram is empty or not. If that is the case, then no other well-formedness checks are performed. If the diagram is not empty, the well-formedness analysis returns: "No errors found" and continues performing the rest of the well-formedness checks.

□ **Goal Single Decomposition**

This check verifies the consistency of goal decompositions. Following the semantics of STS-ml a given goal is decomposed in two or more subgoals. As a result, the decomposition should specify at least two subgoals. Therefore, goal single decomposition verifies whether there are cases of decompositions to a single subgoal.

□ **Delegation Child Cycle**

This check verifies the consistency of goal delegations, so that no cycles or loops are identified as a result of the delegatee decomposing the delegatum (delegated goal) and re-delegating back one of the subgoals. Delegation child cycle verifies exactly this and gives a warning in case of inconsistency.

□ **Delegated Goal Part Of a Decomposition**

This check verifies that all goals (in the delegatee's scope) that have been delegated are not child (subgoals) in the decomposition.

□ **Inconsistent Contribution Cycle**

This check verifies whether there are loops of positive or negative contribution relationships, and whether this loop contains contradictory relationships. If such a loop is identified, the well-formedness analysis returns a warning.

□ **Negative Contributions Between AND Subgoals**

This check verifies that there are no negative contribution relationships between and-subgoals of a given goal (within an actor's scope). It returns a warning if such a case is identified.

□ **Documents PartOf Cycle**

This check verifies whether there is a loop or cycle of Part Of relationships starting from and ending to a given document. If a case like this is verified, a warning is returned enumerating the documents that form the cycle.

□ **Informations PartOf Cycle**

This check verifies whether there is a loop or cycle of Part Of relationships starting from and ending to a given document. If a case like this is verified, a warning is returned enumerating the documents that form the cycle.

□ **Information No Ownership**

This check verifies that all information have an owner. If there are cases of information without any ownership relationships from any actor in the diagram, the well-formedness analysis returns a warning.

□ **Authorizations Validity**

This check verifies that all authorization relationship between two given actors are valid. An authorization relationship specifies authorizations or permissions an actor grants to another on some information, to perform some allowed operations. The authorizations could be limited to a goal scope and they can be re-delegated or not. However, the first two attributes should be specified for an authorization relationship to be valid. If there are no information specified, the well-formedness analysis returns an error. The same applies to the cases, in which no allowed operations are specified.

□ **Duplicate Authorizations**

This check verifies that there are no duplicate authorization relationships, that could be merged. There are several cases that are addressed by this check: (i) we encounter two identical authorization, i.e., between the same roles, in the same direction, for the same set of information, allowed operations and goals, and having the same value of transferability; (ii) identify authorization relationships between the same roles, in the same direction, in which one grants permissions that are subset of the other authorization's relationship.

Appendix C

Details of security analysis:

□ **No_Delegation Violation check**

This violation is verified whenever a delegatee actor further delegates a goal, over the delegation of which a no-delegation security need is specified from the delegator actor. No-delegation is specified over a goal delegation by the delegator, who requires the delegatee not to further delegate the delegated goal. Therefore, to check for any violations of no-delegation, the analysis searches for redelegations of the delegatum (delegated goal) or any of its subgoals.

□ **Redundancy Violation check**

This check verifies if redundancy is satisfied by controlling that single actor redundancy or multi actor redundancy are not violated. At design time we cannot make the distinction between fallback and true redundancy, so they cannot be verified at this stage.Therefore, both fallback redundancy single and true redundancy single are mapped to single actor redundancy. Similarly for multi actor redundancy. The analysis verifies a redundancy violation if one of the following occurs: (1) actor does not decompose the delegated goal in any or-subgoals, for which both types of redundancy are violated (2) actor decomposes the goal into or-subgoals and delegates one to another actor when single actor redundancy has been specified, for which this type of redundancy is violated (3) actor decomposes the goal into or-subgoals, but does not delegate any of the subgoals to another actor when multi actor redundancy has been specified, for which this type of redundancy is violated.

□ **Authorization Conflict check**

This task identifies a conflict of authorization whenever at least two authorization relationships for the same information are drawn towards the same actor from two illegible actors (being the owner of information or another authorised actor) such that: (1) one limits the authorization to a goal scope (requiring a need-to-know security need) and the other does not (authorising the actor without any limitations) (2) for the same goals or intersecting goal scopes, different permissions are granted in terms of operations or authority to transfer authoristaion. That is, one passes the actor the authority to perform operations (use, modify, produce, distribute) on a given information, and the other does not (requiring non-usage, non-modification, non-production, non-disclosure); one passes the actor the authority to further transfer authorizations and the other requires no further authorizations take place.

□ **Non_Reading Violation**

This violation is detected whenever an actor discloses information without having the right to distribute it. Non-disclosure expresses the need of not disclosing or further distributing the given information to other actors, apart from the authoriser. Thus, authority to distribute the information is not passed. The way actors exchange information is through document provision. In order to disclose some information, an actor would have to provide to others the document(s) containing that information. Hence, to verify if there are any unauthorized disclosures of information, the analysis checks for provisions of documents representing the given information from any unauthorized actors towards other actors.

□ **Non_Modification Violation**

This violation is detected whenever an actor modifies information without having the right to modify it. Non-modification expresses the need that information should not be changed (modified), i.e. authority to modify the information is not granted. To verify if there could be any violations of non-modification, the analysis looks if the authorisee (or an actor that is not authorised by authorised party) modifies the given information. For this, it searches for modify relationships from any goal of this actor to any document representing the given information.

□ **Non_Production Violation**

This violation is detected whenever an actor produces information without having the right to produce it. Non-production expresses the need that information should not be produced in any form, i.e. authority to produce the information is not granted. To verify if there could be any violations of non-production, the analysis checks whether if the authorisee (or an actor that is not authorised by authorised party) produces the given information. For this, it searches for produce relationships from any goal of this actor to any document representing the given information.

□ **Non_Disclosure Violation**

This violation is detected whenever an actor discloses information without having the right to distribute it. Non-disclosure expresses the need of not disclosing or further distributing the given information to other actors, apart from the authoriser. Thus, authority to distribute the information is not passed. The way actors exchange information is through document provision. In order to disclose some information, an actor would have to provide to others the document(s) containing that information. Hence, to verify if there are any unauthorized disclosures of information, the analysis checks for provisions of documents representing the given information from any unauthorized actors towards other actors.

□ **NTK Violation**

This violation is detected whenever an actor uses, modifies or produces information for other purposes (goal achievement) than the ones for which it is authorized. Need-to-know requires that the information is used, modified, or produced in the scope of the goals specified in the authorization. This security need concerns confidential information, which should not be utilised for any other purposes other than the intended ones. To verify if there could be any violations of need-to-know, security analysis checks if the authorisee (or an actor that is not authorised by any authorised party) uses, modifies or produces the given information while achieving some goal different from the one it is authorised for. In a nutshell, it searches for need, modify, or produce relationships starting from goals different from the specified ones towards documents representing the given information.

□ **Explicit non-reauthorization**

Verifies whether a given actor transfer rights to others even when it does not have the authority to further delegate rights.

□ **Non-reauthorization Violation: read**

Verifies whether a given actors transfer to other actors the right to use a given information, without having itself the right to do so.

□ **Non-reauthorization Violation: modify**

Verifies whether a given actors transfer to other actors the right to modify a given information, without having itself the right to do so.

□ **Non-reauthorization Violation: produce**

Verifies whether a given actors transfer to other actors the right to modify a given information, without having itself the right to do so.

□ **Non-reauthorization Violation: transmit**

Verifies whether a given actors transfer to other actors the right to distribute a given information, without having itself the right to do so.

□ **Sod Goal Violation**

This violation is detected whenever a single actor may perform both goals, between which an SoD constraint is expressed. Goal-based SoD requires that there is no actor performing both goals among which SoD is specified. To perform this verification, the analysis checks that the final performer of the given goals is not the same actor.

□ **Bod Goal Violation**

This violation is detected whenever a single actor may perform both goals, between which an SoD constraint is expressed. Goal-based SoD requires that there is no actor performing both goals among which SoD is specified. To perform this verification, the analysis checks that the final performer of the given goals is not the same actor.

□ **Agent Play Sod**

This check verifies the consistency of the Separation of Duty (SoD) constraint between roles. This constraint requires that two roles are not played by the same agent, therefore the check verifies whether there is one agent playing both roles. If that is the case an error is identified, otherwise the check finds no errors.

□ **Agent Not Play Bod**

This check verifies the consistency of the Binding of Duty (BoD) constraint between roles. This constraint requires that two roles are played by the same agent, therefore the check verifies whether there is one agent playing both roles. If that is the case the check finds no errors, otherwise an error is identified.

□ **Organizational Constraint Consistency**

This check verifies that no conflicting organisational constraints (SoD or BoD) between goals are specified.