predict
prioritise
prevent

TRESPASS

Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security

Deliverable 7.3.1

Results from Case Study B: Telecommunication Services

Project:	TRESPASS
Project Number:	ICT-318003
Deliverable:	D7.3.1
Title:	Results from Case Study B: Telecommunication Services
Version:	1.0
Confidentiality:	Confidential
Editor:	Ahmed S. Yesuf
Cont. Authors:	Ahmed S. Yesuf, Lars Wolos, Roel Wieringa, Dan Ionita, Margaret Ford
Date:	2014-10-31

Part of the Seventh Framework Programme
Funded by the EC-DG CONNECT

Members of the TRESPASS Consortium

1.	University of Twente	UT	The Netherlands
2.	Technical University of Denmark	DTU	Denmark
3.	Cybernetica	CYB	Estonia
4.	GMV Portugal	GMVP	Portugal
5.	GMV Spain	GMVS	Spain
6.	Royal Holloway University of London	RHUL	United Kingdom
7.	itrust consulting	ITR	Luxembourg
8.	Goethe University Frankfurt	GUF	Germany
9.	IBM Research	IBM	Switzerland
10.	Delft University of Technology	TUD	The Netherlands
11.	Hamburg University of Technology	TUHH	Germany
12.	University of Luxembourg	UL	Luxembourg
13.	Aalborg University	AAU	Denmark
14.	Consult Hyperion	CHYP	United Kingdom
15.	BizzDesign	BD	The Netherlands
16.	Deloitte	DELO	The Netherlands
17.	Lust	LUST	The Netherlands

Document History

Authors		
Partner	Name	Chapters
CHYP	Margaret Ford	4
GUF	Ahmed S. Yesuf	1,3,4,5,A
GUF	Lars Wolos	2,3
UT	Roel Wieringa	3,4
UT	Dan Ionita	1,3,4,5,B
ITR	contributions at a later stage	

Quality assurance		
Role	Name	Date
Editor	Ahmed S. Yesuf	2014-10-01
Editor	Lars Wolos	2014-10-01
Reviewer	Dieter Gollmann	2014-09-11
Reviewer	Frederic Brodbeck	2014-09-11
Reviewer	Alexandr Lenin	2014-09-11
Task leader	Ahmed S. Yesuf	2014-10-01
WP leader	Kai Rannenberg	2014-10-01
Coordinator	Pieter Hartel	2014-10-31

Circulation	
Recipient	Date of submission
Project Partners	2014-10-31
European Commission	2014-10-31

Acknowledgement: *The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TRESPASS). This publication reflects only the authors' views and the Union is not liable for any use that may be made of the information contained herein.*

Contents

List of Figures

List of Tables

Management Summary

Socio-technical systems often have an economic purpose. The current TRE$_S$PASS model handles some economic aspects as shown in the IPTV case study. However, the TRE$_S$-PASS model needs to cover important economic aspects of transactions from different case studies. The case studies described in this report have the aim of identifying relevant commercial aspects of transactions to guide the further development of the TRE$_S$PASS model. For that purpose, case studies from the area of telecommunication services are specified using both the current TRE$_S$PASS model and the e3value business modelling language.

Key takeaways:

- The current version of the TRE$_S$PASS model handles infrastructure-based systems, in contrast to financial aspects (e.g. the money flow between parties).
- From a financial fraud perspective in the telco misuse scenarios, the e3value model better explains the two telco misuse scenarios than the TRE$_S$PASS model. On the other hand, the TRE$_S$PASS model depicts and explains the actors involved in the fraud, the possible actions, the interconnection and the behaviours of actors.
- Both models are of crucial importance for the telco case study. Therefore, to get the full advantages from both models, it is necessary to either integrate the TRE$_S$PASS model with the e3value model, or to have two different models showing alternative views to analyse the fraud in the case studies.

1. Introduction

Under WP7, Task T7.3 is about Case Study B: Telecommunication services. The process for the systematic construction and use of the security model is applied in order to benchmark it in the field of telecommunication services. The task involves multiple iterations and deliverables. D7.3.1 is the first deliverable in applying the telecommunication service case study in different modelling approaches and report the results out of it. In this document, we use the TRE$_S$PASS WP1 model (hereinafter the TRE$_S$PASS model) and the business modelling language: e3value model as the modelling techniques.

From the modelling effort of the two telco case scenarios, we realise that the e3value model captures economic transactions in the telecommunication services better than the TRE$_S$PASS model. However, the TRE$_S$PASS model captures important elements and their behaviour that need to be involved in a successful misuse or attack scenario. We list down the gaps and challenges the current TRE$_S$PASS model has in order for those to be handled in the next development of the TRE$_S$PASS tool.

1.1. Goals

This deliverable D7.3.1 contains results from Case Study B (Telecommunication Services): Case Study B applies the current TRE$_S$PASS modeling approach and the e3value modelling approach on two current scenarios from the of area of telecommunication services which are largely influenced by economic factors. One goal is to find out whether one can model the telco scenarios using the TRE$_S$PASS modelling approach and the second goal is to identify gaps and challenges in the approaches, which will need to be addressed in future revisions and guide the development of the technical work packages.

1.2. Choices made

When producing this deliverable, the TRE$_S$PASS model in (The TRE$_S$PASS Project, D1.3.1, 2013) was still in an early phase. Because of the ambiguities still present in the modelling language, the attack tree generation tool was unable to parse any input other than the sample (IPTV) model file. Thus, a decision was made to manually generate the attack trees (cf. figure 3.2 and 3.4).

In addition, throughout the initial modelling attempts, it was observed that the two misuse scenarios described in Section 2.3 are largely independent of the underlying technical

infrastructure. Furthermore, they come to life as an undesirable result of the complex structure of the tariff plans brought about by the competitive economical environment in which Telecom providers operate. As such, an assumption was made that in order to fully describe the scenarios, a modelling language capable of describing value transactions between actors is required. In order to validate this assumption, a business value modelling language, *e3value* (cf. section 3.2) was selected, as it was thought to be most suitable based on past experiences of the project partners. Generic (non-misuse) business models were created and then the two misuse scenarios were also modelled.

With regard to telecommunication service misuse, there is not much published documentation. This document comes from telco experts and it is based on their experiences. In order to validate the modelling approaches listed in this document, experts from the advisory board assess the modelling approaches and provide a promising initial assessment. Based on this, the modelling approaches are applied using different scenarios.

1.3. Foreground and background

Expert knowledge on the two telco scenarios mentioned in Chapter 2 is considered background and amounts to around 20 percent of the document. The e3value modelling language itself (10 precent of the document) is also background, as it was published in several articles such as Gordijn (2002). The TRE$_S$PASS modelling language, as described in D1.3.1 (The TRE$_S$PASS Project, D1.3.1, 2013), is foreground (10 percent of the document). The e3value and TRE$_S$PASS models created based on the two scenarios, the limitations identified and the cross comparison, as well as the observations, discussion and conclusions are all foreground and they amount to about 60 percent of the document

1.4. Document structure

In Chapter 2 we recap the telecommunication services, the relevant scenarios used in this document and the requirements to model such a case study. This is followed by a discussion about the models using the TRE$_S$PASS model technique and manual generation of attack trees in Chapter 3, which includes also the limitations behind the models. Also, we model the scenarios using the value model technique e3value to complement the limitations of TRE$_S$PASS model and identify the advantages and main limitations of the e3value model. Observations and discussions on the models that came from both techniques are presented in Chapter 4. Chapter 5 describes the main achievements from the models and shows future directions. Appendices A and B at the end contain the screen shots, photos of the discussions in the workshops and coordination model for the e3value model.

2. Case study description

In this chapter scenarios are described which are real world phenomenons in the telecommunications industry. Furthermore, the scenarios are a refinement of the description of the telco scenarios in (The TRESPASS Project, D7.1.1, 2013). Preliminary Results from the modelling of the scenarios using both the current TRESPASS model and the e3value model can be found in Chapter 3.

2.1. About the telecommunications case study in TRESPASS

When taking a closer look, most telecommunications services require a complex technical network architecture. This is due to a multitude of different interconnected networks, service providers and network operators. In most cases the underlying business models are tailored to compete in highly competitive markets. This entails opposed financial interests of the participants and very often even more complex services. Furthermore, this proves fertile ground for fraud or misuse. The rationale behind the choice to place one of the TRESPASS case studies in this specific environment is to enable TRESPASS to include important aspects such as the consideration of business models - or value models or value flows - that deliver incentives for fraudsters and constitute vulnerabilities for the companies involved.

New telecommunication services usually have to be launched under significant pressure, e.g. the requirement of minimizing the time-to-market and to react swiftly to a move of a competitor. This results from strong competition, leaving little time and space to account for potential misuse. Thus, most telecom operators welcome any improvement, if only to implement a more structured approach to reduce the extent of possible misuse, resulting from sloppy (service) design or, whilst knowing about the potential problem, an underestimation or misjudgement of the extent of possible exploitation by fraudsters and their motivation to find combinations of different services, often involving multiple telco operators, which may be exploited.

Expectations of the telecommunications companies from TRESPASS research include the following aspects:

- Identify as many misuse scenarios as possible, in order to find out wether a service is reasonably secure and to minimise potential risks associated with the service (and, as a result, potential losses).
- Preventive solution or technique for dealing with potential fraud related to telecommunications services before it is expoloited (in a large scale).

Thus, TRESPASS can offer an analysis to help improve both the awareness of the company and, as a consequence of this, the robustness of its services in such a competitive environment.

2.2. Definitions and concepts

2.2.1. Telecommunications Service Provider

In the course of the project, the term *telecommunications service provider* with the acronym *TSP* is used. It was chosen in order to cover the different types of providers of telecommunication services.

2.2.2. Knowledge insiders

People who typically exploit their knowledge of the telco or wholesale market for arbitrage practices can be called knowledge insiders. One example of an arbitrage scenario is the use of (flatrate or budget) tariffs for call termination, which will in any case violate the terms and conditions of the respective network operators being misused while usually resulting in a profit for the fraudster.

2.2.3. Types of fraud

In The TRESPASS Project, D7.1.1 (2013), two types of telecommunications-related fraud were distinguished:

- Business case-related fraud
- Fraud related to technical deficiencies

Although this distinction does not prove wrong, it draws off the attention from the fact that, in any case, incentives for fraud indirectly result from the underlying business models (or cases) of the TSPs. Focusing on technical aspects without consideration of the underlying business case perspective would be of little help.

2.3. Fraud scenarios

This section recaps the relevant fraud scenarios used in this document. However, the reader should bear in mind that net loss of a TSP resulting from individual customer's usage patterns is not a problem per se for the respective TSP. In fact, large scale systematic exploitation will add up to a critical level.

Fraud scenario A - Tariff misuse for call termination:

1. Mr. Clever has (multiple) fixed, mobile or virtual IP connection points with TSP A. These are billed either as flatrate or in tariff schemes which include capacious minute budgets.
2. Also, Mr. Clever has (multiple) fixed, mobile or virtual IP connection points with TSP B. Note: Call termination fees are paid on a per minute basis by TSP A when calls are delivered from A to B.
3. TSP B passes a part of the received call termination fees on to Mr. Clever, thereby providing a payout per minute for incoming calls as incentive to generate as much incoming traffic as possible to the B network. Mr. Clever makes calls from A to B in order to maximise his profit from these payouts.

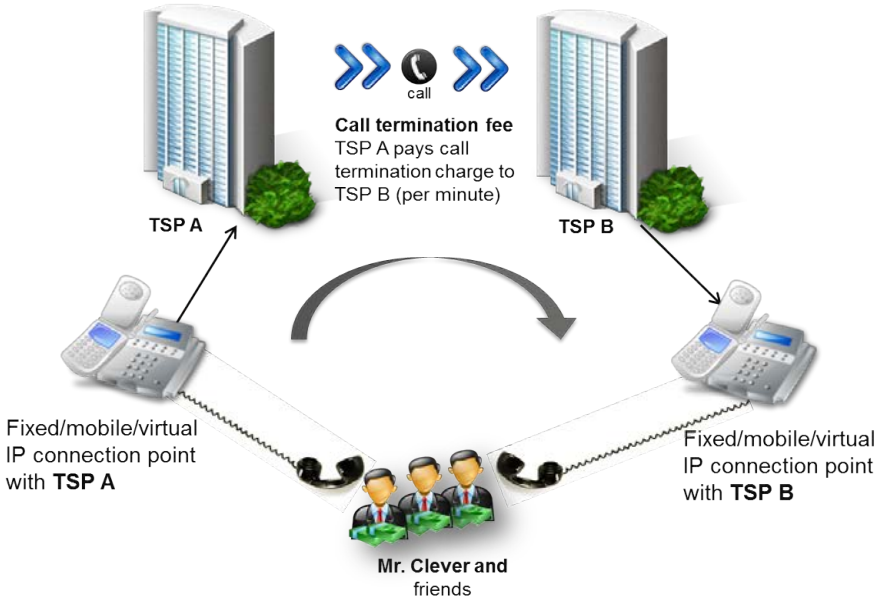

Figure 2.1.: Fraud scenario A - Tariff misuse for call termination.

The source of Mr. Clever's profit is the call termination fee paid by TSP A to TSP B, which is then partly paid out to Mr. Clever by TSP B (Mr. Clever's costs at TSP A are fixed due to the chosen tariff).

Fraud scenario B - fraud involving the false pretence of being willing and able to pay:

1. Mr. Clever obtains a high number of prepaid (pay as you go) SIM cards. These SIM cards are either not (yet) registered or registered using fake or stolen ID. Furthermore, these SIM cards are billed either as flatrate, have a very low price per minute or free minutes (upon activation). In addition to these prepaid SIM cards Mr. Clever manages to establish one postpaid mobile contract with TSP A using fake ID, forged

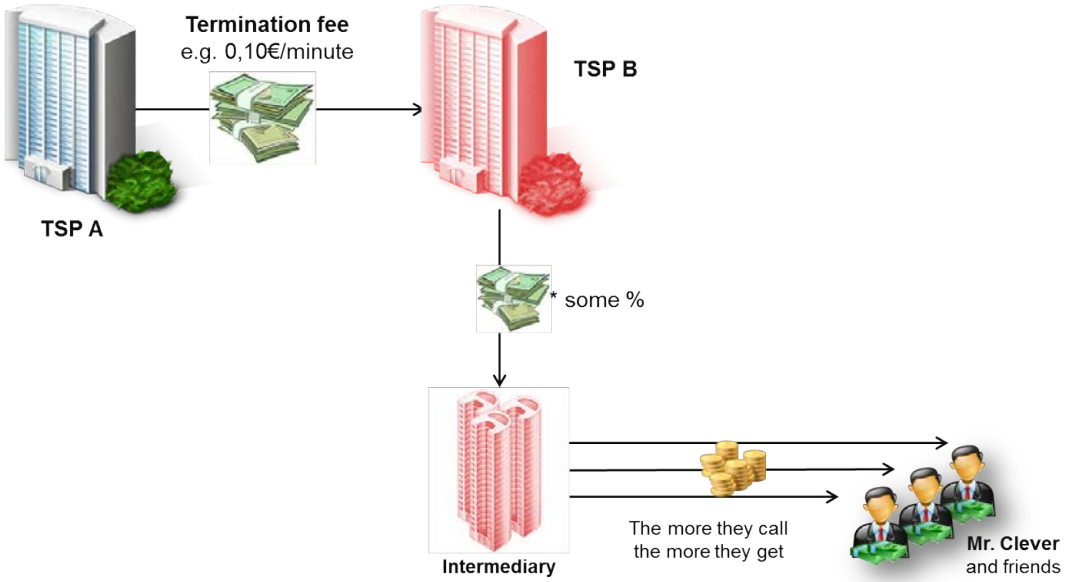

Figure 2.2.: Fraud scenario A - Money flow.

or stolen identity and bank card credentials. Thus, with respect to the postpaid mobile contract, this scenario is a matter of fraud involving the false pretence of being willing and able to pay.

2. Mr. Clever activates *call forwarding* on the postpaid mobile connection point to a (foreign) external TSP B. He then makes the highest number of possible parallel calls to that postpaid mobile connection point using the above prepaid SIM cards. All calls will be diverted to TSP B. Note: Call termination fees are paid on a per minute basis by TSP A when calls are delivered from A to B.
3. The *fraud detection system (FDS)* of TSP A will detect the violation of limits on the postpaid mobile connection contract and disconnect it within the response time.
4. Mr. Clever does not pay the postpaid bill.
5. TSP B passes a part of the received call termination fees on to Mr. Clever, thereby providing a payout per minute for incoming calls.

The source of Mr. Clever's profit is the call termination fee paid by TSP A to TSP B, which is then partly paid out to Mr. Clever by TSP B (outstanding receivables of TSP A will remain unpaid and become a bad debt).

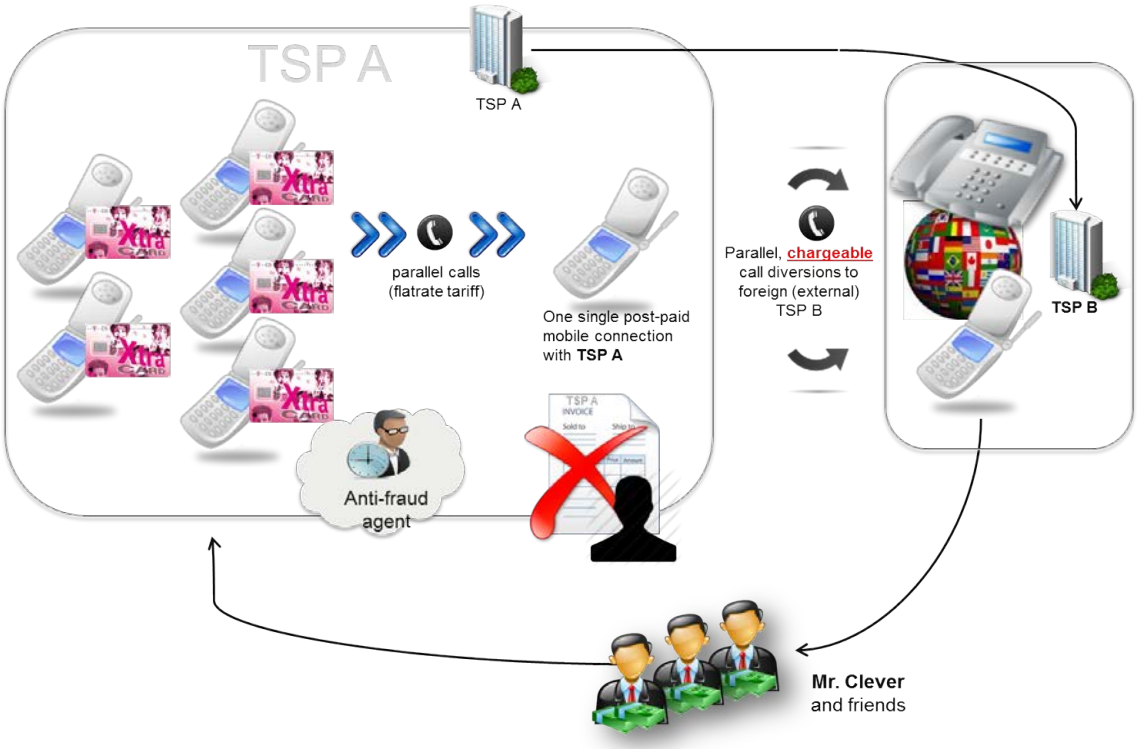

Figure 2.3.: Fraud scenario B - fraud involving the false pretence of being willing and able to pay.

.

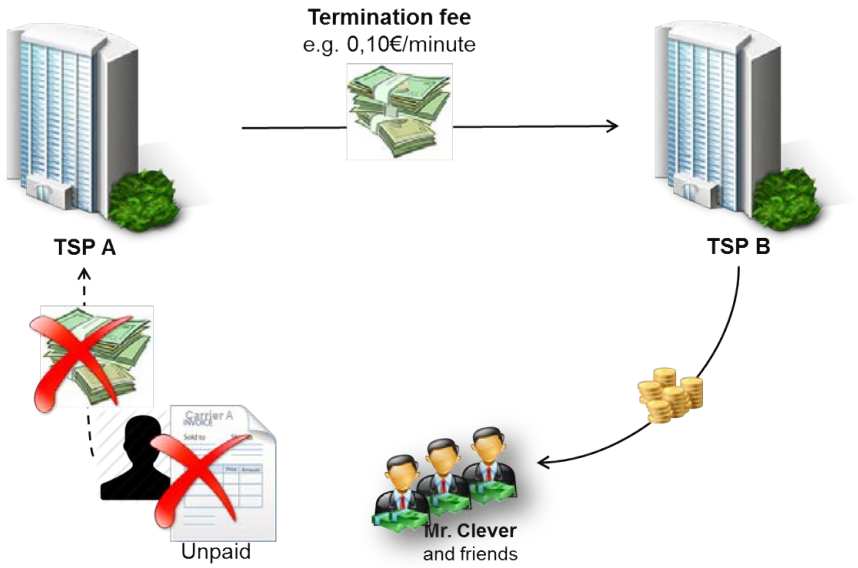

Figure 2.4.: Fraud scenario B - Money flow.

.

3. Preliminary Results

The aim of this chapter is to show how telco case scenarios can be modelled using the current TRE$_S$PASS model and the e3value model. In section 3.1, the two scenarios are modelled using TRE$_S$PASS model. The corresponding attack trees are manually constructed as the TRE$_S$PASS model is still in an early stage, unable to generate attack trees automatically. Considering the current stage of TRE$_S$PASS model development, the e3value modelling approach is applied for the two scenarios in section 3.2.

3.1. TRE$_S$PASS modelling approach

3.1.1. Description

During the course of the project, WP1 is developing a formalism to describe complex socio-technical systems and the attack generation component, capable of generating attack scenarios from navigator maps. Attack scenarios may be presented in various formats: attack trees, attack-defence trees, attack DAGs, and timed automata. At the time of preparing this document, the tool is under development and only the meta-model is used to model the scenarios manually.

One of the essential components of the TRE$_S$PASS model, the navigator map, at its current state represents an organisational infrastructure in terms of nodes and edges in a directed graph (The TRE$_S$PASS Project, D1.3.1, 2013): Nodes represent the locations in the organization that are connected with edges, which can be physical (e.g. door and the corridor), or virtual connections (e.g. the interconnection of two computers via internet). The idea behind such a model is to represent a socio-technical system in a format which makes it possible to automatically generate attack scenarios via policy invalidation (Kammüller & Probst, 2013). One of the representation of such an attack scenario is attack tree. Therefore, the concepts of the infrastructure-based TRE$_S$PASS model are mapped to the concepts behind the telco case, to evaluate the usability of the model: For example, locations in the TRE$_S$PASS model represent doors, rooms or floors, but in the telco case TSPs are modelled as locations.

The main building blocks which are currently available in the TRE$_S$PASS model are mentioned in The TRE$_S$PASS Project, D1.3.1 (2013):

Actors are represented by process nodes, which model all entities that execute a process and may move in the infrastructure. Each actor has an individually defined behaviour, or belongs to a class with a shared behaviour. Actors can share roles,

that can be used in policies. E.g. TSPs and Subscribers of TSPs are considered as actors.

Assets are represented by nodes that can be attached to locations or to actors. Assets attached to actors move around with the actor. Assets model any kind of data that is relevant in the modelled organisation.

Actions are performed by actors or applied to actors. Actions have a target they are performed on. Actions can be logged or unlogged. Receive calls, identify the destination address and transmit the message are, for instance, actions of a TSP.

Policies are used in the TRESPASS model in a rather broad sense; they represent both regulation of access to locations and data, and the behaviour as expected by an organisation from its employees.

3.1.2. Modelling

To model the telco scenarios using the current TRESPASS model, case study partners from WP7 and partners from other WPs are involved in several discussions. In the discussions we:

- identify which entities and issues to include in the model
- identify the connection between the entities
- discuss how to generate attack tree from the models

The original notes from the discussions on this case studies are shown in the appendix A.

3.1.2.1. Entities and issues to model the telco cases

Unlike other case studies, the telco case focuses more on services provided to the customers in terms of products. These products change from time to time depending on the users' need along with the productivity of the TSP. The following entities can be used to model such kind of case study scenarios.

- services
- processes
- pre and post conditions
- parasitic business case measured in terms of cost and benefit

Focusing specifically on the telco scenarios, the TRESPASS model shall include the following issues in the model.

- economic relations

- infrastructures involved
- connection points / telephone calls
- implication on payment entitlements
- risk of not getting paid (for all parties)
- impact on revenue
- lack of ability to control monetary flows
- (legal) domains
- symmetry (e.g. between TSP A and TSP B as mentioned in figure 3.17)
- quantitative parameters in the model
- loss of reputation

3.1.2.2. The models

We show the two models of each scenario and the generate the corresponding attack trees down here.

Scenario 1

The TRESPASS model constitutes modelling of actors, assets, locations, actions, policies and metrics. Figure 3.17[1] shows the first preliminary model using the TRESPASS model. The model has been developed from the workshop discussions.

Telephone A, Telephone B, TSP A and TSP B are the nodes which resemble "actors" in the TRESPASS modelling approach. The connection between these nodes describe the service or money entitlement among the nodes. Additional information annotated as a set of commands alongside each node indicate their functionality. Telephone A and telephone B is owned or controlled by Mr. Clever and their friends.

TSP A:

- in(!CPN): wait for connection to establish (!CPN is an input variable for "called party number", will be bound to phone B in this example)
- out(CPN)@TSP B: establish a connection with the phone "number" in CPN at TSP B (we assume that the CPN is at TSP B)
- out("CTF")@TSP B: pay call termination fee to TSP B
- in("fee")@A: receives the fee for the service A uses; for scenario 2, the fee is not paid by the straw man and this action is not applicable.

[1] The figure is modified from the original figure A.4 (cf. in the Appendix A) to represent only the indicated scenario

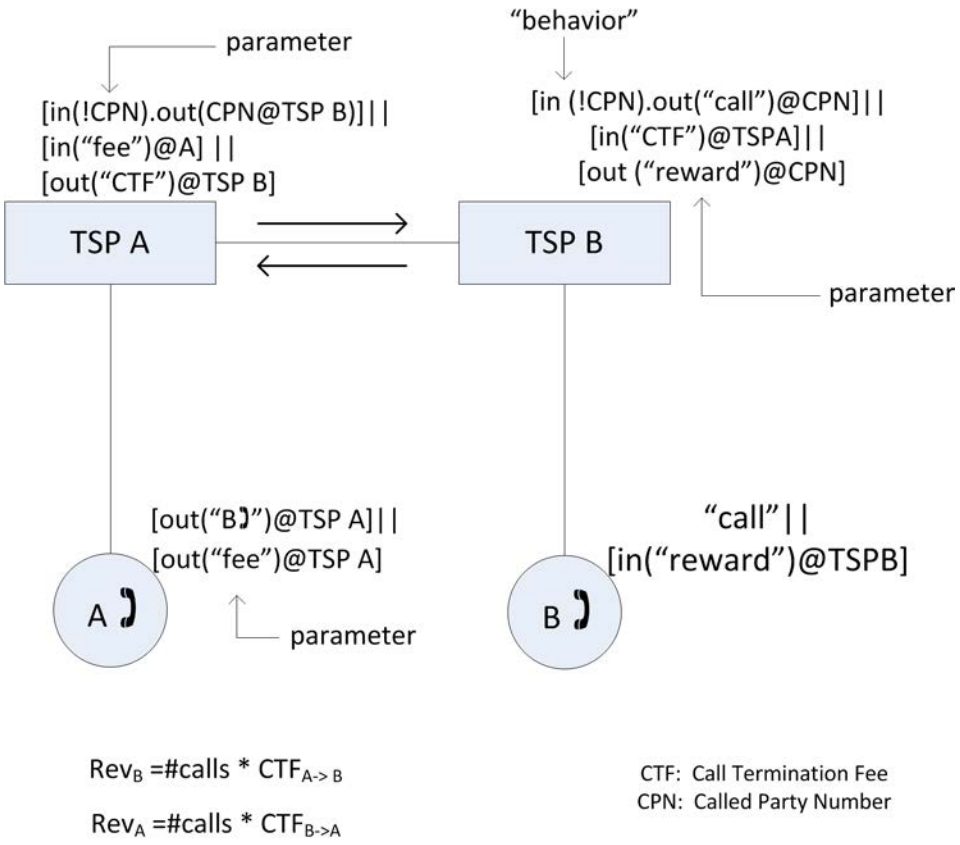

Figure 3.1.: Telco case scenario 1 modeled using the TRESPASS model

TSP B:

- in(!CPN): wait for connection to establish
- out("call")@CPN: notify the phone "number" in CPN of the incoming call
- out("reward")@CPN: this would represent that TSP B makes a payment to the receiver of the CPN
- in("CTF")@TSP A: receives "CTF" from TSP A

Telephone A:

Telephone A is the point of connection where Mr. Clever triggers the call.

- out("phone B")@TSP A: establish a connection with phone B through provider TSP A
- out("fee")@TSP A: pay to TSP A for the call service

Telephone B"

Telephone B is the point of connection where the call traffic from Mr. Clever will be received.

- "call": describes whether the state of the telephone call is accepted or rejected. In this specific scenario, we are interested in "call accepted" state and "call" represented "call accepted" state.
- in("reward")@TSP B: receives "reward" from TSP B

Syntax descriptions of the current TRESPASS modelling approach used in figure 3.17 are shown in table 3.1.

Table 3.1.: Syntax description of scenario1 model

Operators	Description
in	waiting for incoming action
out	outgoing action to other actors
!	waiting for an input e.g. !CPN implies waiting for CPN
dot (.)	sequential actions e.g. in(!CPN).out(CPN@TSP B) implies waiting for CPN and establish connection from TSP B
||	Executing actions in parallel e.g. in(!CPN).out(CPN@TSP B) || [out(CPN)@TSP B] implies executing the two actions in parallel separated with this operator
@	"from" where the action is performed e.g. @TSP B implies that the action is performed on TSP B

Attack tree for scenario 1

The attack tree is generated manually from the model in figure 3.17. The attacker or the abuser in this scenario can be legal customers who have a subscription agreement with a TSP. The goal of the abuser (from phone A) is to gain exceeded profit by generating a lot of traffic to TSP B. To achieve this goal, 1) find suitable TSP (in this case TSP B) 2) establish agreement with TSP B and 3) Launch the attack. As the attack tree is shown in figure 3.2, the three sub-goals are further refined to achieve the root goal.

Scenario 2

The entities involved in this scenario are TSPs, subscribers of TSPs (Telephone A and B) and the forwarding Telephone S.

Mr clever owns multiple pre-paid phones (Telephone A) and he controls the middleman, which is to some extent equivalent to ownership. There is a challenge to model the concept of ownership (cf. refer to section 3.1.3)

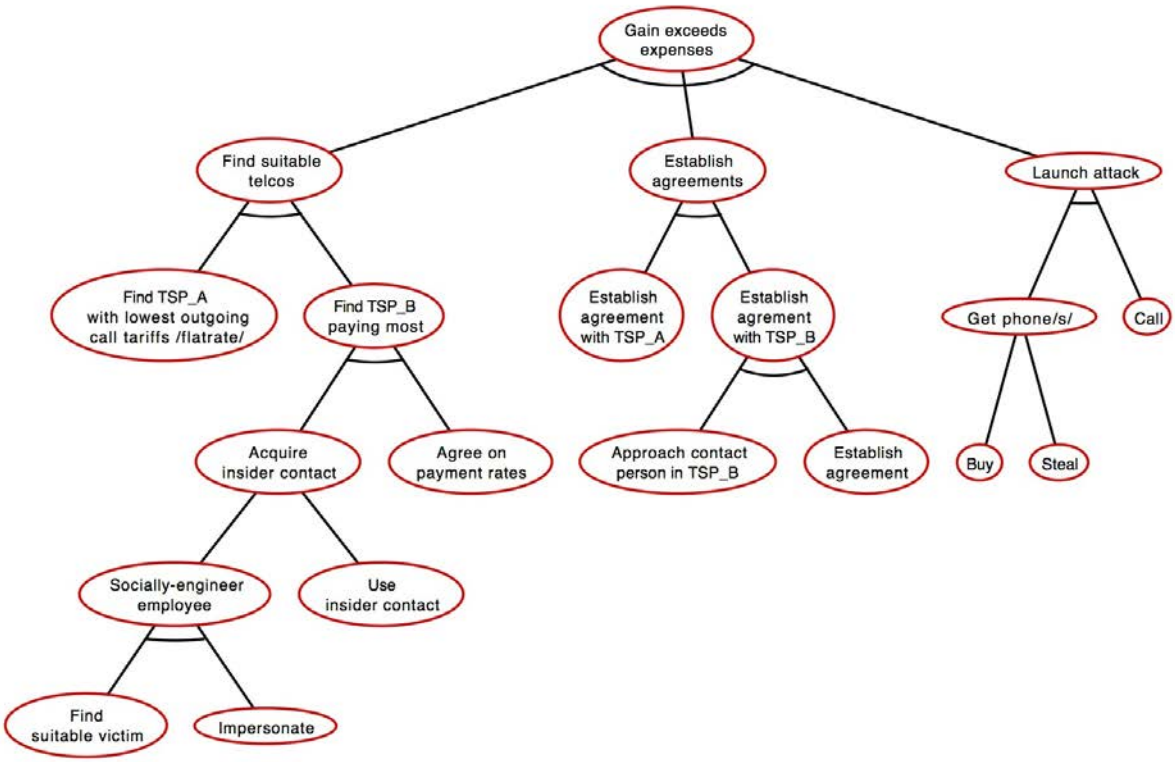

Figure 3.2.: Attack tree for scenario 1

Attack tree for scenario 2

The goal of the attack tree for scenario 2 (figure 3.4) is to get money or not paying for the contract. The attacker has three sub-goals to achieve the main goal: 1) find numbers, which have a lot of payout, from TSP B 2) setup the forwarding phone and 3) generate calls (to get money out of call termination). Each of this sub-goals are refined down to leaf nodes (attacks). To setup the forwarding phone, an attacker can either finds a postpaid phone out of jurisdiction, hack the forward server or social engineer the employees of TSP A. Stealing SIM, credit card, find straw man to sign a contract are the possible attacks to find a postpaid phone.

The attack trees in both scenarios show that the potential attacks or misuses happen to the customers, the employees of a TSP and the TSP itself in order to gain money. Furthermore, such combined attacks towards the customers of a TSP or TSP employees lead to the misuse of the TSP services. These attack steps are represented in the attack trees.

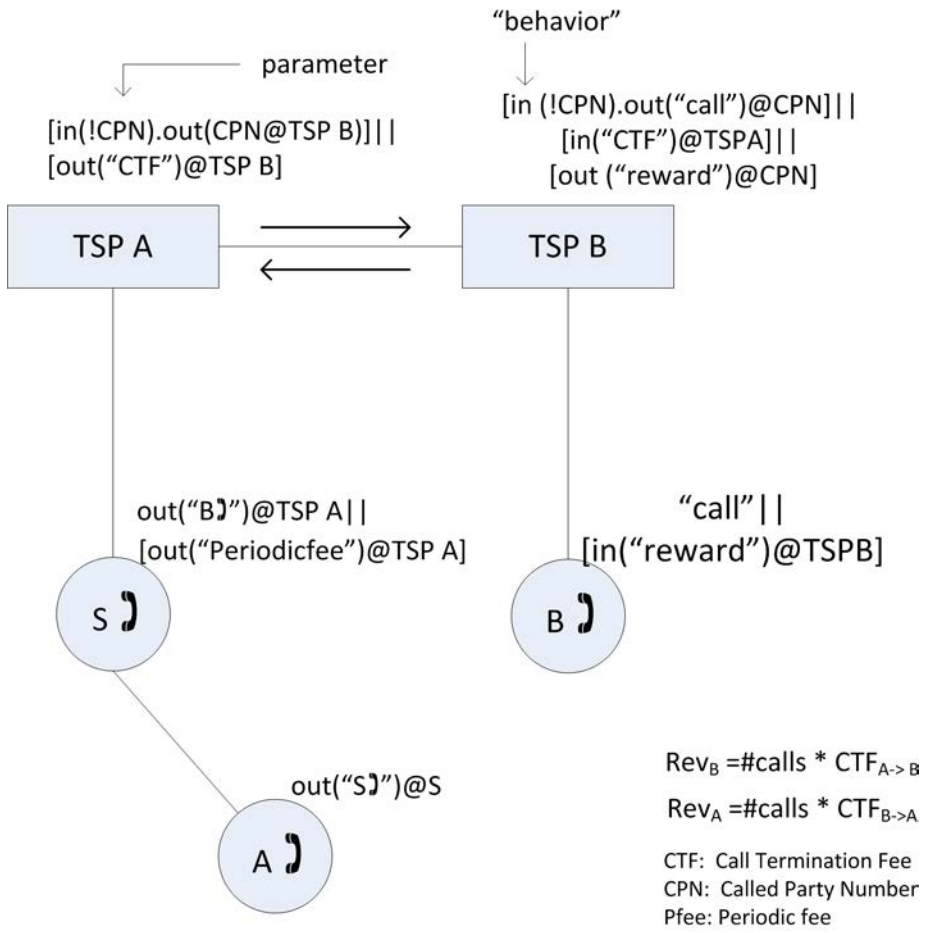

Figure 3.3.: Telco case scenario 2 modeled using TRESPASS model

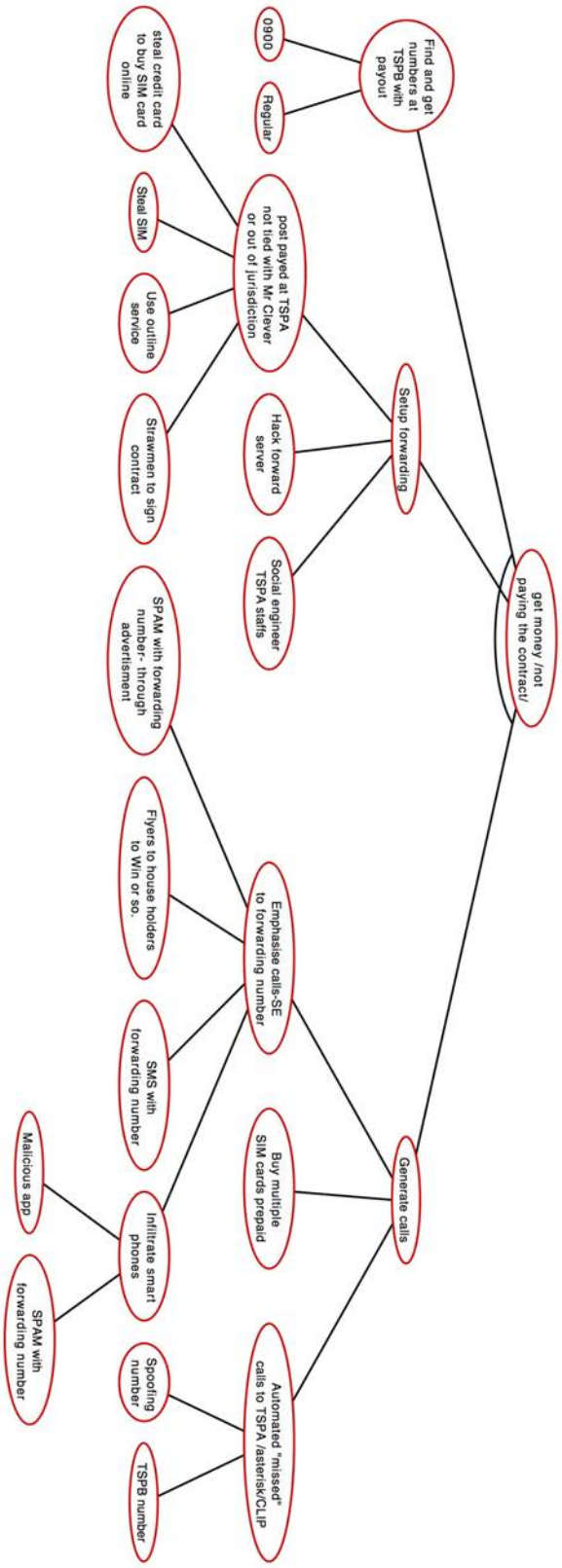

Figure 3.4.: Attack tree for scenario 2

3.1.3. Limitations

This section describes the limitations of the TRESPASS modelling approach at its current stage.

3.1.3.1. Ownership of entities

As of the current level of development, the ownership of entities has not yet been implemented. The concept of ownership implies that entities (such as e.g. mobile phones) are purchased, possessed and used (controlled) by other entities (e.g. Mr. Clever).

3.1.3.2. Agreements between entities

As of the current level of development, agreements between entities have not yet been implemented. For example, the attacker Mr. Clever may have an agreement with a TSP. Furthermore, in this case the information about the existence or details of the agreement would normally be hidden from other entities in the model. Thus, only Mr. Clever and the respective TSP are aware of it. Thus, agreements may be key to the model, enabling attacks (without the agreement between Mr. Clever and the TSP there would be no economic basis for it) while also indicating and explaining the attacker's behaviour.

3.1.3.3. Scalability

With respect to scalability, there are some issues to be resolved. On one hand, modelling large amounts of same or different entities, is yet to be tested. A large amount of entities could be e.g. a huge number of

- prepaid SIM cards or phones,
- different payout schemes or call routes,
- different actors or, generally, parties with some economic interest involved, or
- a multitude of possible (new) activities from a technical point of view (in terms of behavioural patterns of an attacker).

On the other hand, scalability also refers to the ability to handle scenarios that have a bigger overall scope.

The e3value model able to model, for instance, how many SIM cards or phones generate call traffic to TSP B. It is also possible to indicate what type of payment contracts Mr. Clever posses with TSP A: prepaid or prepaid. Thus, the e3value model is scalable and flexible in this regard.

3.1.3.4. Money budget of entities

As of the current level of development, money budgets (budget restrictions) for entities in the model have not yet been implemented. These budgets are needed in order to account for the fact that attack scenarios

- will quickly be scaled up to an efficient (short-term) maximum by an attacker depending on attacker's budget, attacker's assumptions regarding the risks involved, and necessary physical hardware resources readily available at the attacker's disposal,
- are subject to multiple kinds of limitations of the respective service (these limitations may relate to service design aspects, availability, wholesale- or identity-related restrictions, and others).

In order to understand the thoughts and ideas behind the above aspects, consider a budget or "call volume" granted to a (new) user. Limitations from the product side, such as e.g. the number of parallel connections possible, may also be reflected by a budget. Furthermore, restrictions regarding network access and acceptable usage patterns might be imposed on new users by a TSP: Stronger restrictions regarding acceptable flat-rate use or fair use policies during initial trial or usage periods of prepaid SIM cards may apply until identity or credit checks or the corresponding registration process as a whole for a new customer has completed.

3.1.3.5. Less dynamic

The model does not depict all the dynamic aspects of the telco case. For example, the money flow is mentioned in terms of "reward" that will be paid when a customer (e.g. Mr. Clever) has an agreement with TSP B. It is not clear how to model such type of conditional nature of the case. Another example: It is difficult to know "how much" money the attacker will earn from a successful attack (misuse). In other words, the money flow is integrated abstractly for the attacker to simulate and find out how much profit can get.

The main functionality of the e3value model is representation and computation of economic value flows between economic actors involved. It computes how much money Mr. Clever earns from a successful misuse scenario and how much money a TSP losses or gains because of a successful misuse scenario. This makes the e3value model ideal for the telco scenarios that involve economic flows. The e3value model has also its own limitations, which are discussed in section **??**.

3.2. e3value modelling approach

In order to overcome the limitations of the current TRE$_S$PASS model (cf. section 3.1.3) and incorporate into the next iteration of the TRE$_S$PASS tool development, we took a value modelling approach: e3value, as an alternative approach. It is because the e3value model

supports modelling of the money flow, entitlement and ownership of entities found in the two scenarios. The following sections describe the e3value language and tool and present the modelling results. Finally, conclusions are drawn with regard to the applicability of e3value in particular – and value models in general – to the modelling and risk assessment of Telecommunication fraud scenarios.

3.2.1. Description

The e3value modelling language was first introduced by Gordijn (2002) in order to support better understanding of the economic transactions occurring in an e-commerce environment, where a constellation of profit-loss responsible entities create, exchange and consume things of economic value. In other words, "the e3-value methodology provides modelling concepts for showing which parties exchange things of economic value with whom, and expect what in return" (Gordijn, Akkermans, & Van Vliet, 2000).

Figure 3.5 shows the buidling blocks of e3value and a simple example, showing the commercial relationships between the publishers of a number of newspaper tiles, their advertizers and and their readers. The main building blocks available in the e3value toolkit, as depicted in Figure 3.5, are:

Actor is an independent entity capable of exchanging value. They can represent a person, market segment, business or role.

Value object is something of value to at least one actor, which can be exchanged with other actors, such as services, products, money or even customer satisfaction.

Value port is used to represent the ability or desire of an actor to provide or request value objects. It allows to abstract away from the internal business processes in order to focus only on the external interaction between actors.

Value interface – groups together two or more value ports belonging to the same actor. It shows what an actor is willing to offer in return for a a certain value object.

Value exchange – connects two value ports from different actors together as to show the flow of value objects between actors

Value offering – is a group of value exchanges in opposing directions used to show reciprocal value exchanges between actors.

Dependency path – is a chain of value offerings, starting from a Start stimulus and ending in one or more end stimuli that shows which value offerings occur and when.

Start stimulus – is a need of one of the actors to acquire a certain value object. Connection elements are used to define which transactions are triggered by each occurrence of the need.

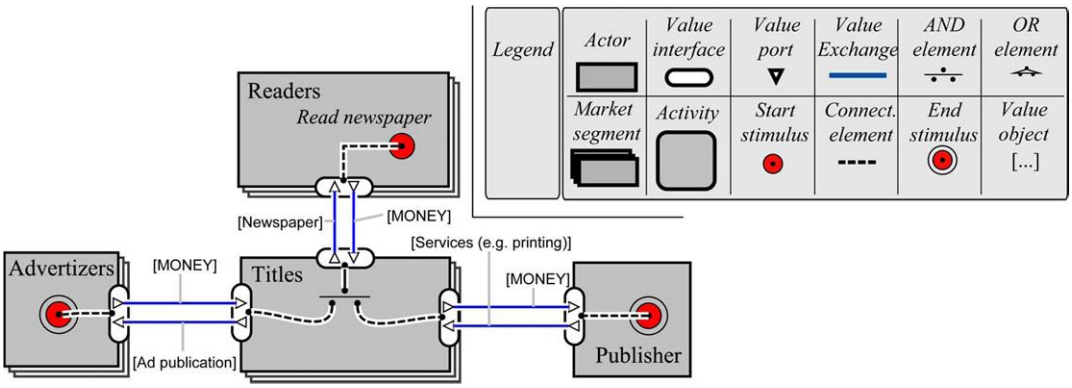

Figure 3.5.: Example and legend of an e3value model

Looking at Figure 3.5, we observe that Readers have a need ("Read newspaper"). What the model then shows is that for each occurence of this need (each Reader that decides he wants to read a nwespaper), some money is paid by this reader in exchange for a newspaper to the a Title (an independent news paper). For each such purchase, some money is also cashed in from an Advertizer in exhannge for exposure. Furthermore, as depicted by the end node, for each such purchase an amount of money is forwarded to the publisher in exchange for a service (e.g. printing). A single Publisher might own a number of such Titles, which he sees as profit-loss reponsible business units. The purpose of the publisher is to share facilities that require economies of scale, such as printing, logistics and IT, and to share facilities related to personnel, finance, etc. Such services are provided to the Titles in exchange for a (part of) the income they receive from Readers and Advertizers.

Ocurence rates (i.e. average number of times a need is expected to occur per contractual period) are assigned to Start Stimuli. Valuations (i.e. quantifications of the monetary value of each value object) are defined as properties of Transactions (if both stakeholders assign the same value) or Ports (if each stakeholder assigns a diffrent value for the same object). Fractions (smaller or larger than 1) can be assigned to AND/OR nodes such as to allow for the following transactions to be triggered a proportional number of times.

The occurrence rates of a start stimulus determine the number of occurrences of each Value Exchange on the same dependency path. My multiplying the number of occurences of each Value Exchange with the valuation of it's associated Value Object, the tool is able to calculate the incoming/outgoing money flows of each actor. These money flows can the be added up to show the profit/loss each actor stands to make per contractual period. By running this analysis a large number of times, for different occurence rates of the same need, we are able to generate various profitability graphs, such as the one shown in Figure 3.9.

However, it is important to remember that the order is which transactions occur along a dependency path does not necessarily represent the sequence of activities in real life. Value models are not process models: they do not describe how processes are carried out or by whom.

Supplementary conventions

While creating value models of the mis-use scenarios, it was observed that in order to model fraud or misuse correctly, supplementary modelling conventions are needed. This is because we need to be able to represent hidden or unexpected transactions. It is exactly these transactions that commonly form the basis for of such fraud scenarios. To mitigate this, we introduce three types of value exchanges:

1. Normal: These value exchanges take place as expected.
2. Dashed: These transactions occur in the world, but are not observable to at least one of the actors.
3. Dotted: These transactions are expected to occur, but will not.

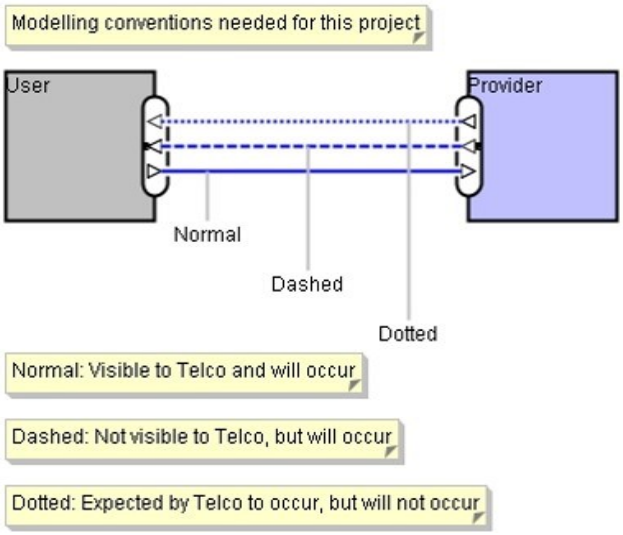

Figure 3.6.: Newly introduced e3value transaction types

3.2.2. Modelling

As a first step, a generic (non-malicious) scenario was created which shows the various payment plans commonly available to customers of TSPs: pre-paid, post-paid and flat-rate. This was done in order to get an impression as to how these various tariff plans could be modelled in e3value.

Next, two models were created for each scenario: one only showing the expected value transactions and one including hidden or unexpected transactions which enable financial gains by malicious customers. We call these two alternative models *views* as each shows the same value model from the perspective of one of the actors. The first one will show the situation as it is expected by the TSP (as our target of assessment). The second one will provide a view of the same scenario, but including hidden transactions that only the attacker is aware of.

Assumptions

An important assumption used when creating the models is the following: in each model (except the base case) only a single payment plan is taken into account. This is because, although a variety of other plans which influence the profit of the TSP exist, we are interested in the impact and risks of a specific (new) plan.

A second important assumption is about the behaviour of users. Since it would be infeasible to model an infinite amount of user behaviours, we limit ourselves to at most two types of users per model: malicious and non-malicious. We use averages to describe their behaviour. Of course, their parameters can be tweaked to, for example, conduct sensitivity analysis of the results or create best/worse case estimations.

Finally, when constructing the models, we used numbers provided by GUF to parametrize the models. These numbers are shown in Table 3.2.

Table 3.2.: Average values used for payment plans

	Pre-paid	Post-paid	Flat-rate
Initial payment	€5,00	€0,00	€0,00
Monthly payment	€0,00	€10,00	€37,5
Cost per minute	€0,03	€0,10	€0,00
Minutes included	334	-	∞
Note	Double minutes as welcoming bonus	-	∞, until fair use policy is reached
Interconnection fee		€0,07/minute	

3.2.2.1. Base case

The base case attempts to describe the complete environment of the TSP, from a service provision perspective. Obviously, this model is not exhaustive and only provides an overview of the possible relationships between TSPs and their customers by modelling the most common payment schemes found in the Mobile Telecom sector. The resulting e3value model is shown in Figure 3.7.

Users A1-A3 are used to model different types of payment plans. In that sense, they do not represent individual users but customer types:

User A1 is a user with a normal post-paid plan. This means that once a month the base rate needs to be paid. When this user makes a call, an extra cost occurs which user A1 promises to pay. This payment will be made at the end of the period.

User A2 has a pre-paid plan. For each minute of calling, the costs that that occur are deducted from the user's account immediately. Most of the time this is done through some kind of crediting system.

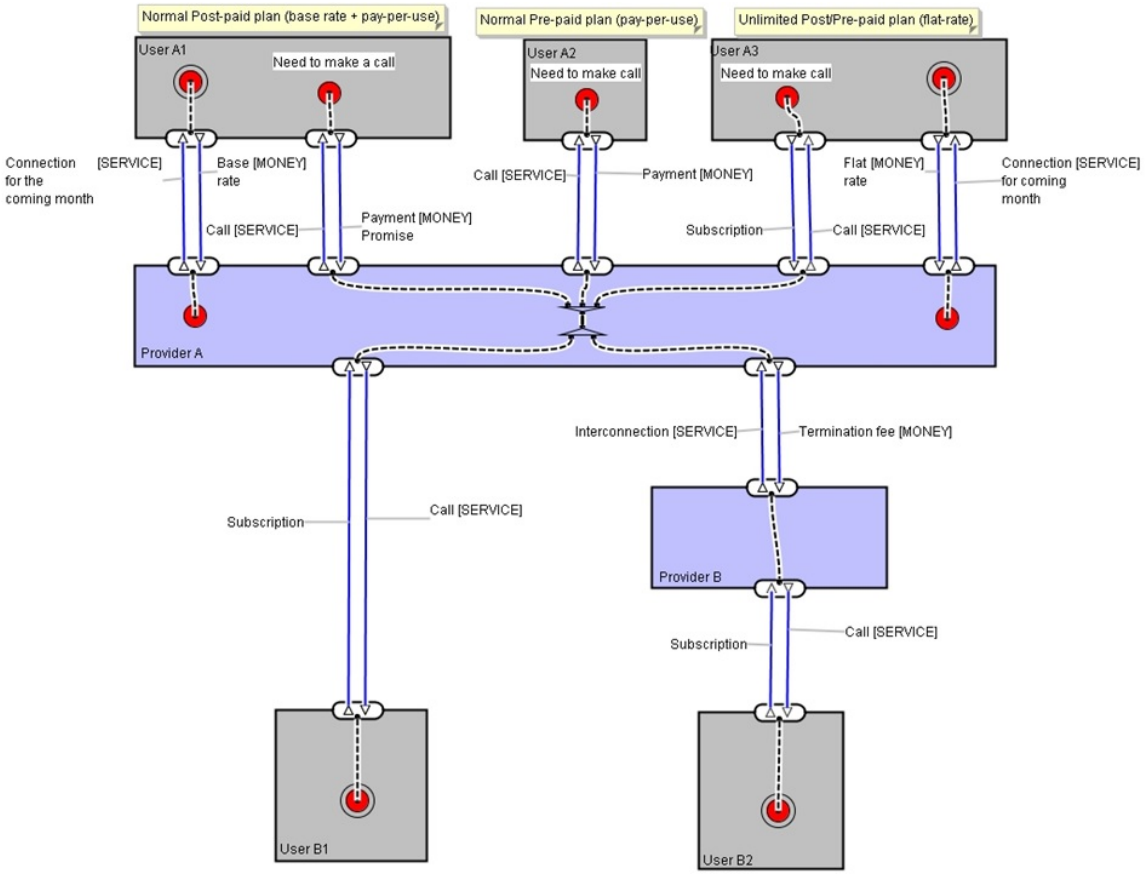

Figure 3.7.: Base case - e3value model

User A3 describes customers with flat-rate plans. This means the user pays a fee once a month and after this unlimited calling becomes available to him. In order to make a call, the only thing needed is his subscription.

In the middle of Figure 3.7, TSP A is used to represent the TSP from whose perspective the model is created. This is important as there is a potentially endless constellation of actors that could be added to the model. However, we choose to only include those actors and transactions that could potentially influence the profitability of the plans offered by our target of assessment (TSP A).

In the bottom of the figure we position the receivers of the calls that the customers of TSP A are placing. In that sense, User B1 and B2 also represent a role: that of users receiving a call initiated from the network of our target of assessment (TSP A). They can be either part of the same network (i.e. User B1) or could be customers of another network (i.e. User B2). Note that since a person could have multiple contracts with various TSPs (or even the same TSP), it is possible that two or more of the roles depicted in the Figure (A1-A3 and B1-B2) could be fulfilled by the same physical person.

3.2.2.2. Scenario 1

The first misuse scenario is based on double-contracting. Firstly, Mr. Clever has a contract with TSP A who provides him cheap with the ability to perform cheap calls. This can be any type of contract but, as shown below, a flat rate contract is the best way to make a profit. Secondly, Mr. Clever needs a contract on which it is profitable to receive calls. This contract could, for example, provide him with a bonus fee for each minute of calling he receives. In order to avoid detection, this contract would probably be with another TSP (TSP B).

For this scenario to be profitable for Mr. Clever, the bonus fee he receives from TSP B needs to be bigger than the rate he pays to TSP A. This is why a flat rate plan is his best option. As this plan has a fixed payment per month with unlimited minutes, the minute rate of this plan goes down the more minutes he uses. Of course this only works until the limit of the fair use policy is reached. The real limit of this policy is unknown, but for this research 1500 minutes per month is assumed within the limit.

Telecom TSP's view The model in Figure 3.8 shows the scenario described above. User A3 has flat rate contract with TSP A. User B2 has a contract with TSP B. As TSP A is not expecting any deviation, there is no problem in User A3 calling User B2. Just an ordinary call. The expected financial result of TSP A (Y-axis), relative to the number of minutes called by User A3 (X-axis) is shown in Figure 3.9.

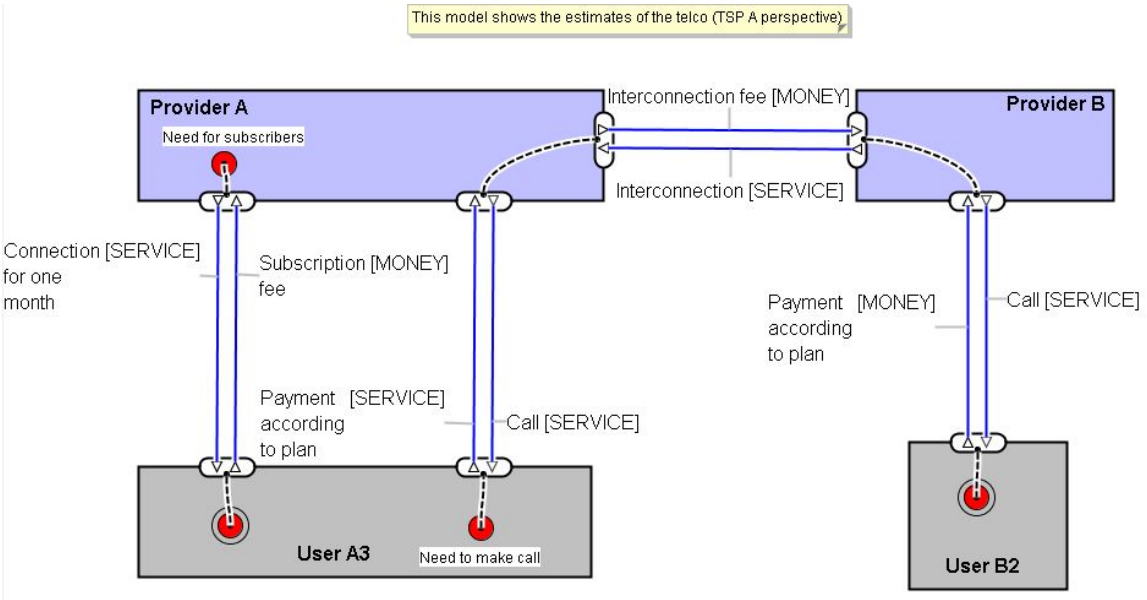

Figure 3.8.: e3value model of scenario 1 - TSP A view

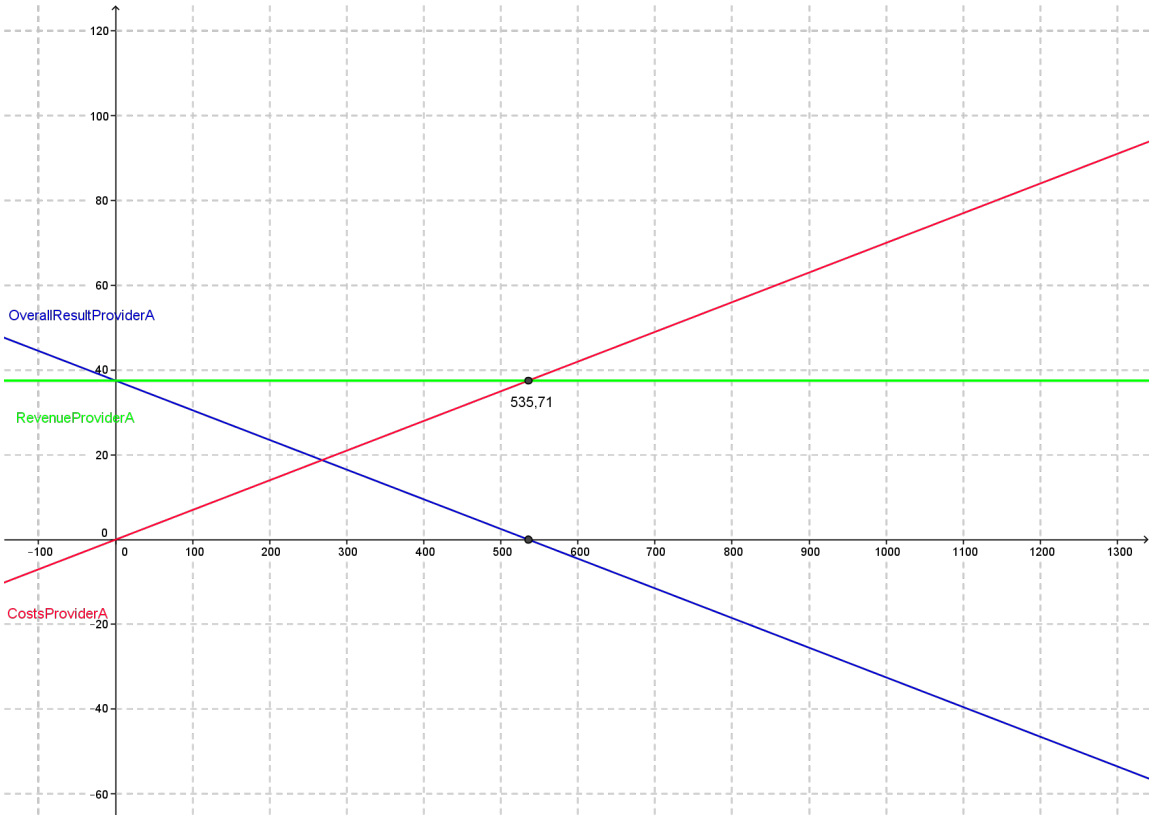

Figure 3.9.: e3value profitability computation for TSP A - TSP A view

Mr Clever's view In Mr. Clevers plan, shown in Figure 3.18, things are slightly different. In his perspective, user A3 and B2 are the same person (or at least working together). A clause unknown to TSP A in User A's contract with TSP B is introduced. User A gets €0,055 per incoming minute as a bonus for generating traffic. This puts User A (a.k.a. Mr. Clever) in a potentially profitable position. In order to achieve profit, Mr. Clever needs to make calls for less than €0,055 per minute. This can be reached because of the flat rate plan. The more minutes are used, the cheaper they become per minute. The expected financial result of Mr. Clever, again relative to the number of minutes called, is shown in Figure 3.11.

3.2.2.3. Scenario 2

The second scenario has some similarities to the previous scenario, but involves an amplified attack using re-directed calls. Mr. Clever starts by finding a middle man, which is willing to take a post-paid contract in his name. This step will probably require some form of payment (assumed €50). When the middle man has acquired the SIM card, it is immediately forwarded to a foreign number and switched off.
The foreign number to which it is forwarded, is also part of the scenario. Mr. Clever again has a contract with TSP B and again gets a bonus fee for every incoming minute. The last

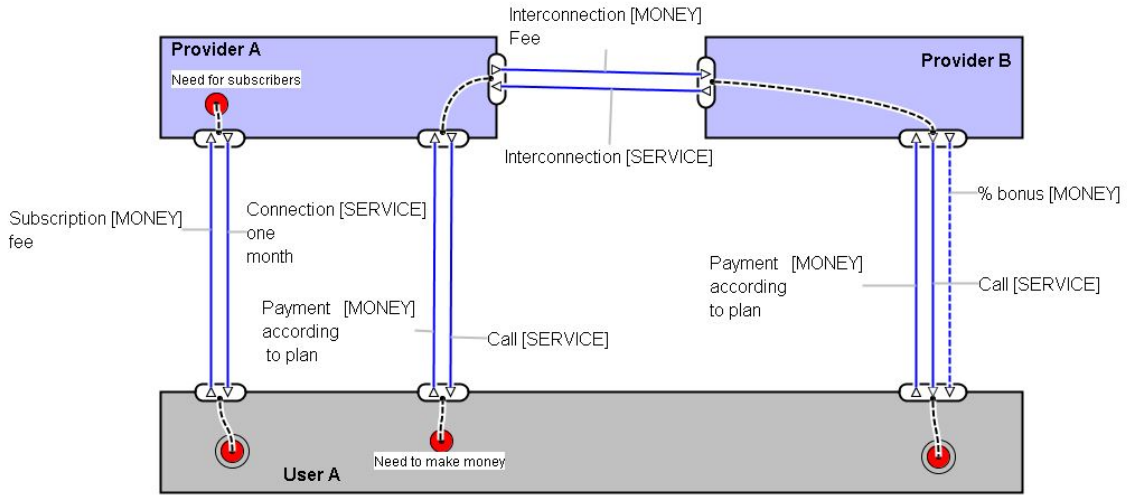

Figure 3.10.: e3value model of scenario 1 - Mr. Clever view

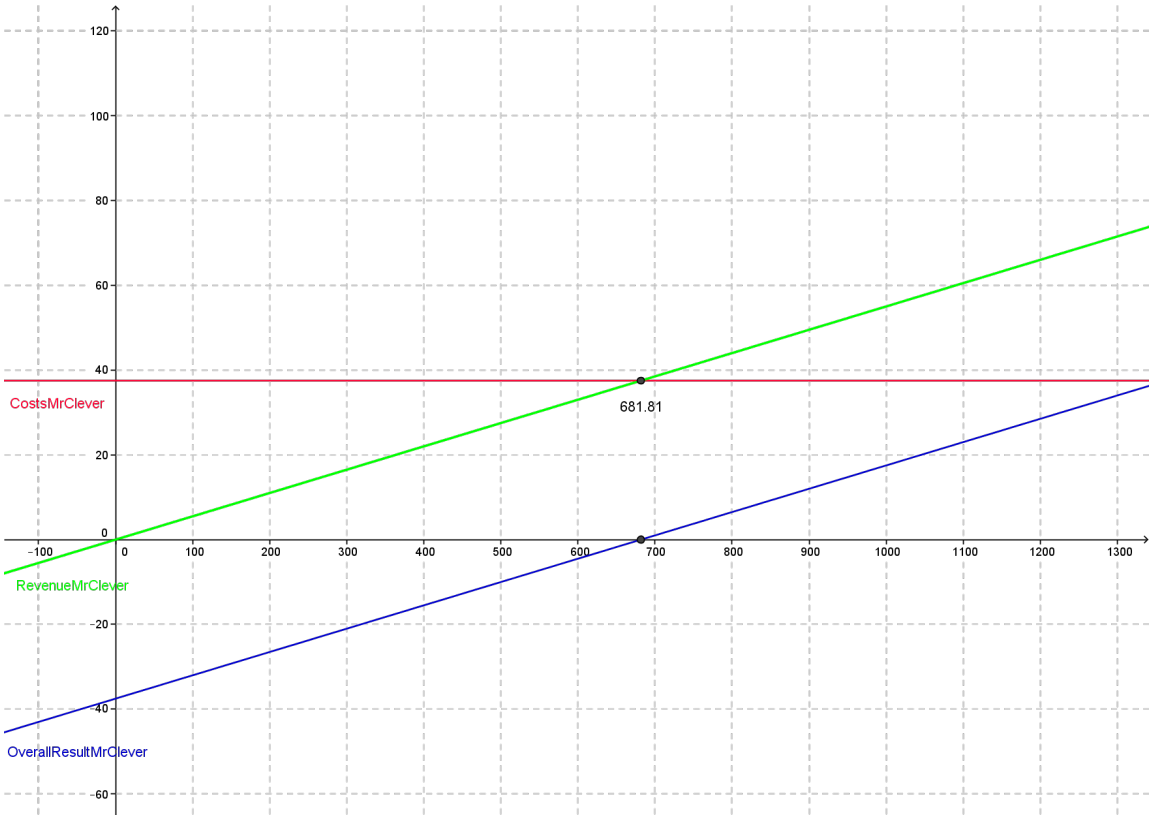

Figure 3.11.: e3value profitability computation for Mr. Clever - Mr. Clever view

thing Mr. Clever needs is some incoming calls. To generate these he acquires a set of prepaid (anonymous) SIM cards from the same TSP as the postpaid.
To make money from this, Mr. Clever uses his prepaid cards to call the postpaid number.

This can be done for low costs as they are with the same TSP. As the postpaid number is forwarded, the calls get forwarded to the abroad number at TSP B and Mr. Clever gets paid from there. The number of prepaid cards used directly amplifies both the potential profit for an attacker and the potential loss for the TSP.
When creating these models, a coordination model was first created to get a better understanding of the process involved . This was done because this scenario has some clear phases that need to be completed in a specific order. For example, the phone number needs to be forwarded before the calling starts. By putting the scenario in an activity diagram, all steps become clearer and can be checked against the e3value model. It became clear that a connection between two swim lanes in the activity diagram, was represented by a transaction in the e3value model. The coordination model is shown in Appendix B (FigureB.1)

TSP's view Figure 3.12 shows the perspective of TSP A (as the target of assessment). In this scenario, User A buys a prepaid card, pre-loaded with 334 minutes of credit as a welcoming bonus. With this credit, User A can make calls. On the right side, User MM has a postpaid plan. The expected financial result of TSP A is shown in Figure 3.13.

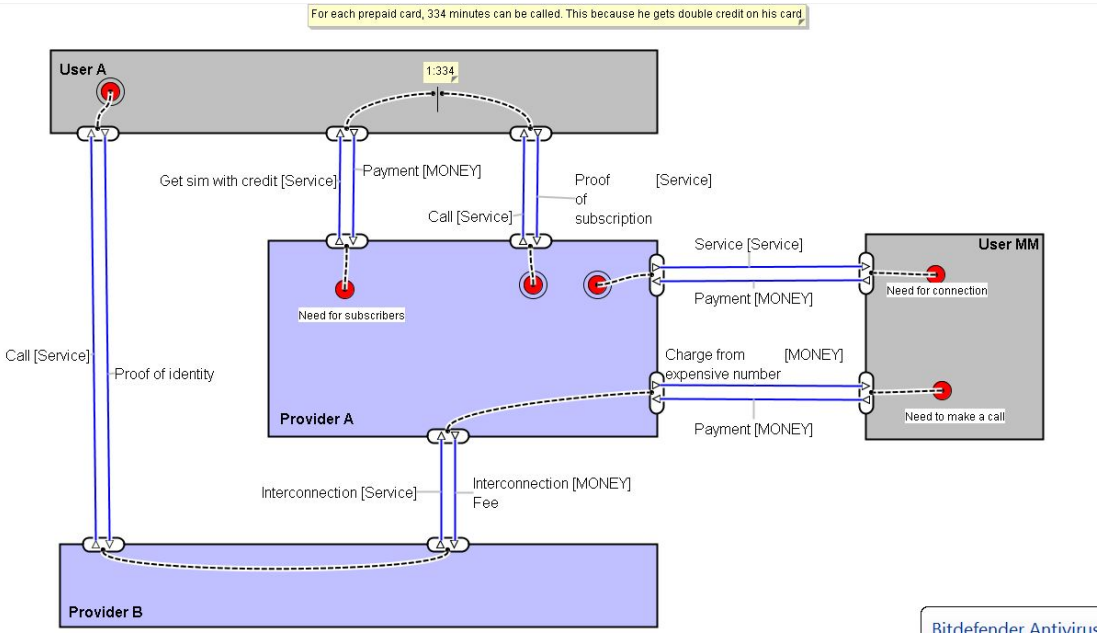

Figure 3.12.: e3value model of scenario 1 - TSP A view

Mr Clever's view In Figure 3.14 the business case of Mr. Clever is shown. Noteworthy are the new hidden transactions appearing between User A and User MM and User A and TSP B respectively. Furthermore, the two payments for the post-paid are now dotted (non-occurring). Similarity to scenario one, this gives Mr. Clever the opportunity to make a profit by exploiting the unintended interaction between the two contracts. The expected

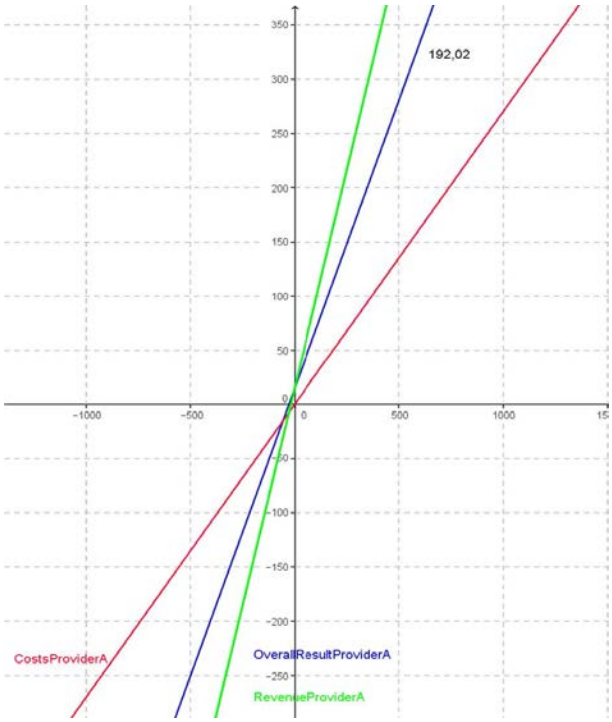

Figure 3.13.: e3value profitability computation of scenario 1 for TSP A - TSP A view

financial result of Mr. Clever, for various amounts of pre-paid SIMs is shown in Figure 3.15. Note that while for a single SIM card Mr. Clever will not make a profit due to the high initial investment of paying the middleman (MM), his profits explode once over ten SIMs are used simultaneously. A reciprocal graph showing the massive loss TSP A would face if User A is acting maliciously is shown in Figure 3.16. If Mr. Clever was only to use 20 SIM cards these losses might amount to over €5000 for one month. Of course, this income gained from non-malicious users should also be considered, as the TSP might still make a profit if only a small percentage of users acts maliciously.

3.2.3. Limitations

Based on the e3value models, the profit or loss for both the TSP and Mr. Clever could be calculated. Furthermore, break-even points for all actors can be derived. These calculations were made based on data from several sources. However information about the current workings of a TSP was obsolete. Assuming the modelling is undertaken by the TSP itself, the computations and models would become more accurate. This however, has no influence on the method used to calculate these profits.

The fact that e3value does not recognize any kind of order in its execution, is one of its strong points. But in some cases the order in which the transactions happen is important. For example, its impossible to make a call with a SIM card that hasn't been bought yet. The how question (critical to process models) does not concern us, but the order in which

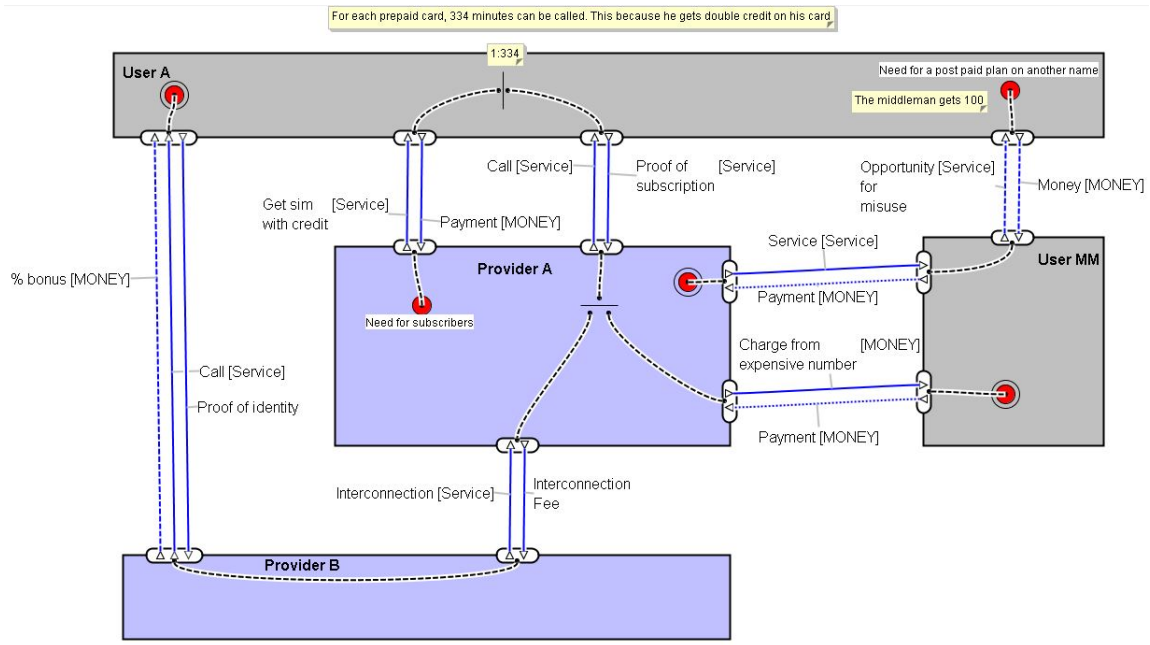

Figure 3.14.: e3value model of scenario 2 - Mr. Clever view

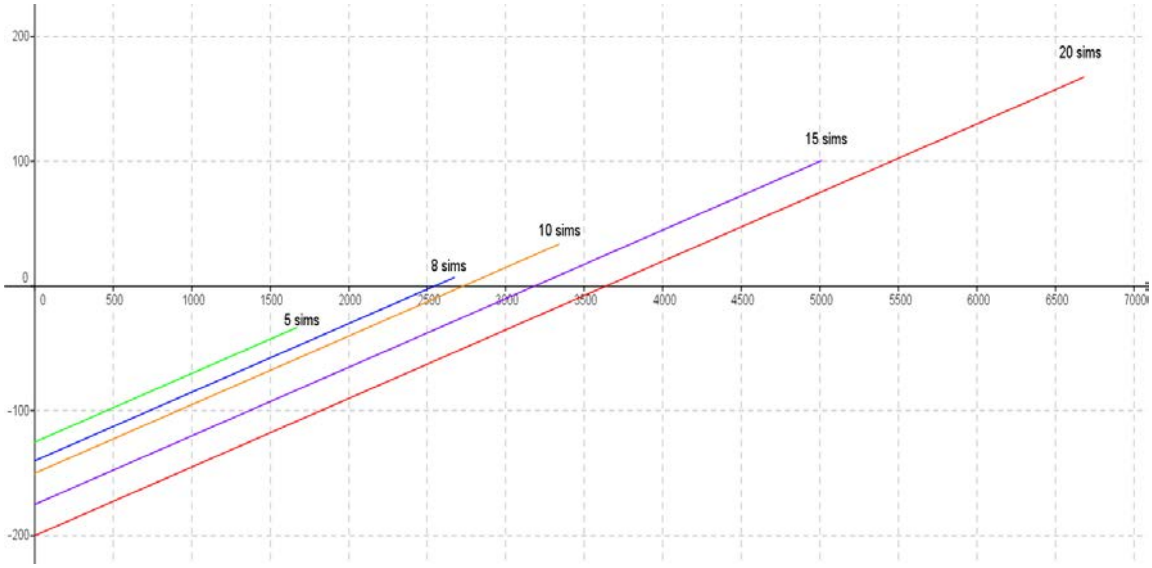

Figure 3.15.: e3value profitability computation of scenario 2 for Mr. Clever - Mr. Clever view

certain transactions are executed does matter. This was solved with the use of an activity diagram, but if a language is created for fraud detection, some way of specifying a high level order is a requirement.

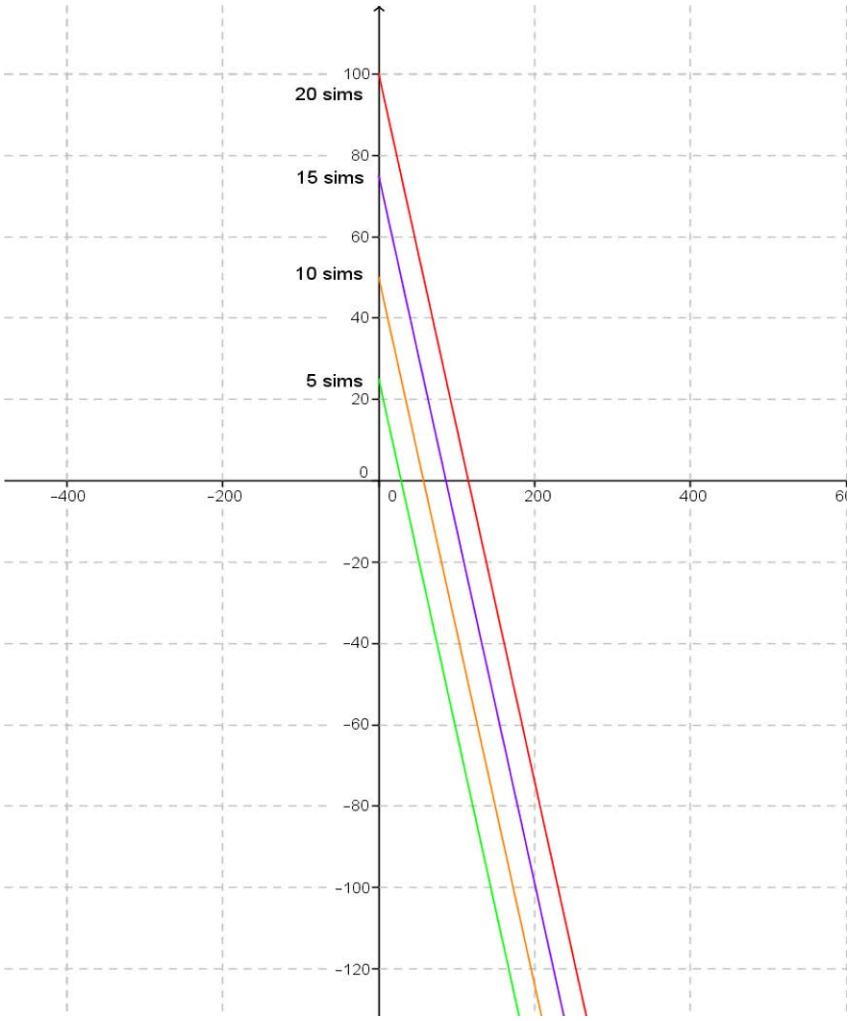

Figure 3.16.: e3value profitability computation of scenario 2 for TSP A - Mr. Clever view

In e3value, all transactions have to be reciprocal. However, a characteristic of fraud is that sometimes nothing is given in return. This was currently mitigated by using transactions of null value.

A limitation of the e3value toolkit is that it can only compute profitability graphs for a static set of parameters. To mitigate this, the e3value computations were ran multiple times and formulas were extracted which allowed the creation of the profitability graphs based on a parameter like number of minutes talked or number of SIM cards bought. In order to allow for sensitivity analysis and determining the impact of various factors on the profitability of the plan, it is essential that the future model be able to create such graphs automatically.

Finally, in order to be usable in a Risk Assessment process, a method of automatically identifying opportunities for misuse for a given tariff plan is needed. A possible solution would be to create a sufficiently large number of fraud scenarios and then train a pattern matching algorithm to determine if any of those can occur on a given model. However, this

assumes a substantial effort in creating the library and would not work very well for new types of fraud. An alternative would be to generate non-ideal scenarios by: (1) merging actors, (2) Making payments non-occurring (like not paying subscription fee at the end of the month) and (2) adding hidden transactions (like the bonus

3.3. Cross-comparison

This section focuses on placing the two models described in the previous sections side-by side in order to highlight the commonalities and differences between the two approaches. The next page shows the two models next to each other allowing a quick comparison, while the following paragraph will summarize some obvious differences and similarities.
We can quickly observe that there are a set of common entities in both models. While collusion between callers A and B is not represented in the TRE$_S$PASS model, the two figures contain almost the same actors. However, the TRE$_S$PASS model struggles to represent the money flows as in/out operations while completely omitting several other value exchanges which actually explain these money flows (such as the needs that trigger them, the services or products traded in exchanges, the dependency between these various exchanges or the visibility of these flows).

Furthermore, while the TRE$_S$PASS model allows for the generation of an attack tree describing the steps needed to accomplish the attack, the e3value model allows for the plotting of estimations of impact for the TSP and gain for the fraudsters against several parameters. These provide different types of information, which might be useful in different (Risk Assessment) scenarios, the details of which are to be further investigated.

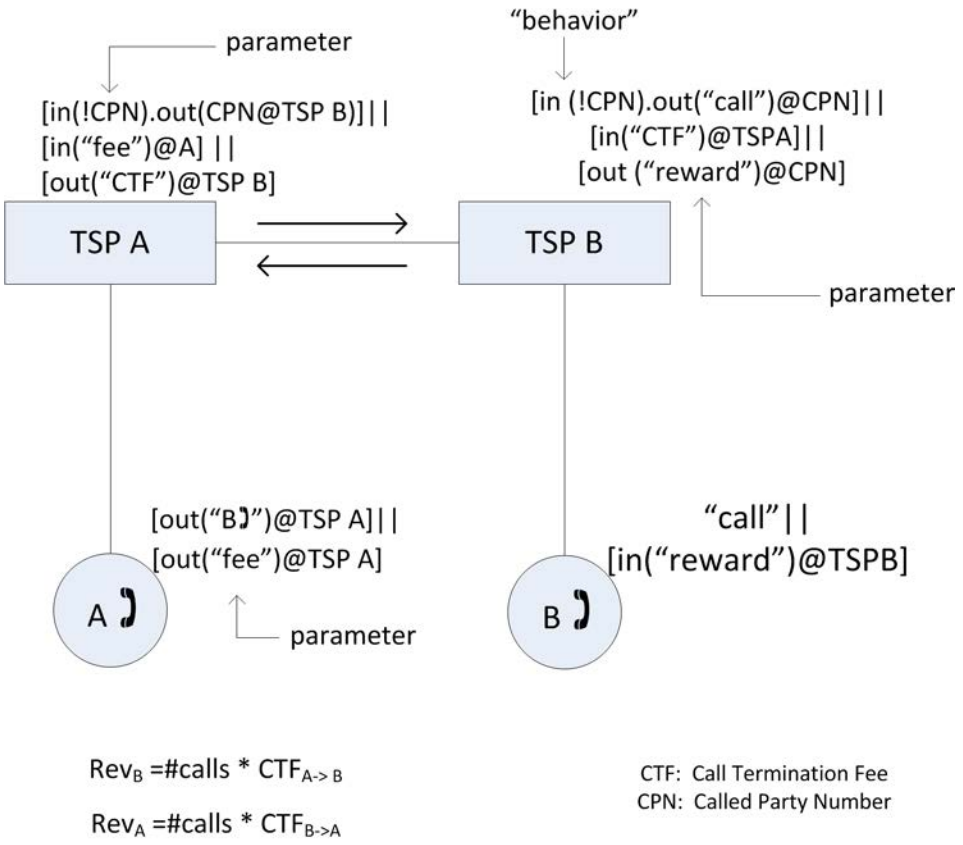

Figure 3.17.: TRE$_S$PASS model of scenario 1

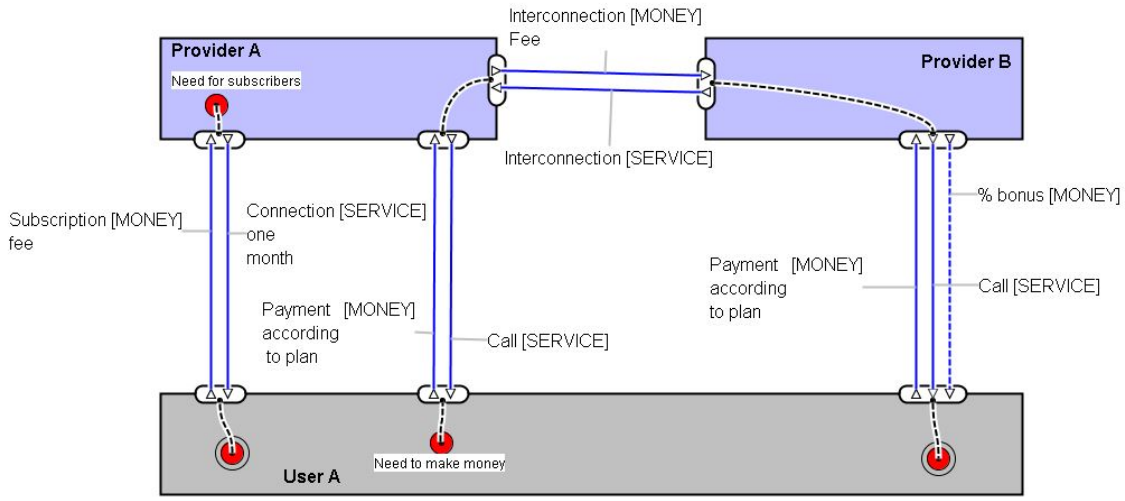

Figure 3.18.: e3value model of scenario 1

4. Observations and Discussion

4.1. Architecture models vs. value models

The current TRESPASS model represents the target of assessment as a set of interacting components. The represented components are software, hardware, people, or social systems, and the relations among components are access relations. In that sense, it is a (socio-technical) architecture model.
Value models like e3value, on the other hand, represent only business transactions in a declarative way: The components are profit-and-loss-responsible actors, i.e. businesses, business units, or consumers. The relations among components are exchanges of value objects, where a value object may consist of money, goods, services, or even experiences (e.g. music). This can be the same system as represented by an architecture model, but focusing only on the value aspect.

A key difference between the two is that actors in e3value models are economic actors, i.e. profit-and-loss-responsible businesses, business users, or consumers. Actors in the TRESPASS model can be any individual or even represent an abstract role.

While both models describe the same socio-technical system, they present almost disjunct views. This implies that while a small set of consistency relationships can be defined between the two, they essentially contain different information, thus making transformations impossible. The feasible and/or useful set of such consistency relationships is left for future investigation, as described in Section 4.3.

4.1.1. Applicability

The biggest strength of e3value models is also their biggest weakness: they abstract away from any and all procedural and architectural information. This makes such models easier to use and understand by non-technical people. Furthermore, they are specialized in describing money flows.
For Case Study B (Telecommunication Services), and especially for the two scenarios described in this document, this makes them ideal: information on the technical infrastructure is un-obtainable, the process is very simple and the actual attack path almost irrelevant. Describing the money flows and their triggers is necessary and sufficient to describe the scenarios and not only derive estimates of both impact for the provide and gain for the fraudsters, but also identify countermeasures.
However, if we are interested in (preventing) the technical exploits that allow the attack

to happen, or want to reason about the timing, ordering or the possible attack vectors involved in the attack, more information is needed. This information is not obtainable from an e3value model. As such, for other scenarios such as Case Study A (IPTV), where the attack involves technical exploits or social manipulation, not only will a socio-technical model be needed, but might also be sufficient.

Based on feedback from industrial Telecom partners and practitioners, we have identified two application scenarios for e3value models: (1) assessing financial magnitude of fraud on a new plan before it is launched and (2) estimating impact of newly discovered fraud possibilities on existing plans.

The above brings about the question of deciding when and where each type of model is needed in order to conduct an effective Risk Assessment. This question is to be tackled in future deliverables, as indicated in Section 4.3. Furthermore, it now becomes crucial to find ways by which this variety of models can work together in an integrated (TRE$_S$PASS) work-flow. This is also briefly discussed in Section 4.3.

4.2. Observations on model creation

The current TREsPASS model is well suited to the customer privacy protection (IPTV) case study, in that it deals with people, machines and data in a space which can be reasonably well defined both physically and logically. The cloud case study equally has strong technical aspects which are well suited to the socio-technical model being developed in WP1. While there are physical and technical elements to the telco case study and there may be value in exploring both physical and technical countermeasures, the fundamental challenges it presents are commercial. As such the case study is best understood through a modelling process that can highlight the complexities of the commercial environment.

Telco fraud cases are not really attacks but misuse cases. Misuse cases are not necessarily against the law or even against contractual or usage agreements, as they do not involve tampering with the normal operation of devices or exploiting vulnerabilities in their operation. So the actions in a telco fraud case are not part of an attack, and are not aimed at accessing an asset owned by a telco. However, these actions may impact the revenue of the TSP as this behaviour deviates significantly from the TSP's exectations and/or estimations. If we view a contract between actors in an e3value model as a policy, then the goal of Mr Clever is to find a way of misusing these contracts to his own advantage, in a way that usually is not intended by the telcos. His actions are governed by telco contracts. In the two scenarios modelled, no knowledge of vulnerabilities in IT infrastructures was needed.

Timing is extremely important in relation to this specific case study: the marketing department of a telco will want to launch their products without delay and so any kind of initial analysis of prospective risks arising from proposed products will need to be comprehensive enough to be meaningful and yet quick enough to be acceptable. Once the product

is launched, it will be important to identify any unacceptable activity at the earliest opportunity, to minimise the losses associated with this. If information is available from previous misuse scenarios, there may also be some value in investigating the delay between launch and increasing levels of misuse as a partial predictor of future expectations.

4.3. Future Work

This deliverable only presents the results and observations of the first attempt at using e3value models to complement the current architecture and coordination models available in TRE$_S$PASS and overcome the obstacles encountered especially in the Telecommunication Services Case Study. Despite showing promising results, there is still a lot left to investigate with regard to the utility, usability and applicability of such models as well as with regard to their relationship to existing models, approaches and tools.

A main topic of research for the coming year is investigating how value models can be integrated in to the TRE$_S$PASS workflow. It is already obvious that they do not contain sufficient information to allow for the generation of attack trees. As most of the TRE$_S$PASS tools developed so far rely heavily on this attack representation structure, they are not compatible with e3value models. Furthermore, since transformation to or generation of any sort of architecture or coordination model (TRE$_S$PASS or otherwise) from an e3value model is not feasible (Gordijn et al., 2000), new ways have to be devised to allow exploiting the information available in these models such that it can be used in the TRE$_S$PASS workflow. One option would be generating the root node of an attack tree from an e3value model: each undesire-able transaction could be decomposed into atomic actions needed in order to achieve it, thus forming a (sub-)attack tree. Another, simpler option would be simply using e3value models for impact and gain estimation, leaving the other analyses to be performed on more technical models.

A secondary research topic, party stemming from the above, has to do with investigating and fleshing out the formal or otherwise relationships between value models and architecture or coordination (process) models. There exists previous work discussing these relationships , such as Singh (2013); Janssen, van Buuren, and Gordijn (2005); Gordijn and Van Vliet (1999) and Wieringa and Gordijn (2005); Pijpers and Gordijn (2007); Gordijn and Wieringa (2003), respectively. However, none of these papers are about (in-)security or fraud and mostly assume ideal business environments. As such more focus should be attributed to identifying the (consistency) relationships which are relevant or useful in the context of Risk Assessment and the specifically, the TRE$_S$PASS project.

5. Conclusions

Overall, we have observed that e3value models better captured economic transactions of the two misuse scenarios modelled, compared to the TRE$_S$PASS model. Furthermore, e3value was somewhat easier to create as less knowledge about the technical infrastructure was needed and the building blocks and syntax was simpler. In this sense, it not only overcame several of the TRE$_S$PASS (WP1) language constraints but also provided more flexibility and ease of use when discussing telco fraud.

However, we do expect that for similar attacks, which (also) exploit technical or social vulnerabilities, e3value models will not be sufficient. Such technical vulnerabilities may be exploited in scenarios involving hacking of a TSP's or TSP customer's infrastructure (e.g. CPE - Customer-premises equipment, PBX - Private Branch Exchange). In this case, an integrated model, describing all relevant aspects of the scenario or two different models showing alternative (but potentially overlapping) views would be necessary. Considering the fact that being able to only create one type of model would in some cases increase usability while decreasing complexity, as well as similar indications received from the Advisory Board, it seems the latter version is preferable. This, of course, brings about the issue of deriving complex attacks, risks, and respective countermeasures from these two different models in a consistent and meaningful way. For the project, this means that during the next year, the possibility should be explored of generating Attack Trees, Timed Automata or whatever other attack representation is chosen from e3value models, in addition to the established TRE$_S$PASS model.

In addition, there may be an opportunity to apply the approach used here in a wider context. In particular, there could be opportunities to explore the social implications of parasitic business models as described in this document. There is a wide range of different applications of this type of study. In this telco case study, it involves the abuse of the system in order for an individual to profit from loopholes in the contracts offered by TSP's. However, there are many other circumstances under which the study of parasitic business models may be valuable.

Apart from those who profit from abusing the services offered, there is also the widespread problem of 'free riders', those who benefit from features of particular services to obtain those services at a reduced cost or no cost at all. This is an area of very great interest to the major transit providers, who are obliged to monitor their systems constantly to keep track of the ways in which a proportion of travellers short circuit the controls in place.

Although these activities may not be criminal, some of the approaches to social data based on Crime Science being developed in WP2 might be of value in understanding these types of behaviour. These look at the motivations of the attacker and the ways in which the

owners of the system may endeavour to reduce the extent of the harm done. This can include looking at patterns of behaviour and the effectiveness of specific interventions.

6. References

References

Gordijn, J. (2002). *Value-based requirements engineering: Exploring innovatie e-commerce ideas*. Unpublished doctoral dissertation, Vrije Universiteit Amsterdam.

Gordijn, J., Akkermans, H., & Van Vliet, H. (2000). Business modelling is not process modelling. In *Conceptual modeling for e-business and the web, ecomo 2000* (Vol. 1921). Springer.

Gordijn, J., & Van Vliet, H. (1999). On the interaction between business models and software architecture in electronic commerce. In *Addendum to the proceedings of the 7th european software engineering conference/foundations of software engineering / esec 1999.*

Gordijn, J., & Wieringa, R. (2003). A value-oriented approach to e-business process design. In *Proceedings of the 15th international conference, caise 2003* (Vol. 2681, p. 390-403). Springer Verlag.

Janssen, W., van Buuren, R., & Gordijn, J. (2005). Business case modelling for e-services. In D. R. Vogel, P. Walden, J. Gricar, & G. Lenart (Eds.), *Proceedings of the 18th bled conference (e-integration in action)* (p. cdrom,). Maribor, SL: University of Maribor.

Kammüller, F., & Probst, C. W. (2013). Invalidating policies using structural information. In *Ieee symposium on security and privacy workshops* (p. 76-81).

Pijpers, V., & Gordijn, J. (2007). Bridging business value models and business process models in aviation value webs via possession rights. In *Proceedings of the 20th annual hawaii international conference on system sciences* (p. cdrom). Computer Society Press.

Singh, P. M. (2013, August). *Integrating business value in enterprise architecture modeling and analysis.* Retrieved from http://essay.utwente.nl/63695/

The TRE$_S$PASS Project, D1.3.1. (2013). *Initial prototype of the socio-technical security model.* (Deliverable D1.3.1)

The TRE$_S$PASS Project, D7.1.1. (2013). *Initial requirements for implementation of case studies.* (Deliverable D7.1.1)

Wieringa, R., & Gordijn, J. (2005). Value-oriented design of correct service coordination protocols. In *Proceedings of the 20th acm symposium on applied computing* (p. 1320-1327). ACM Press.

A. Discussion on Whiteboard

Figures A.1, A.2, A.3, A.4, A.5, and A.6 are outcomes of discussions and are shown below.

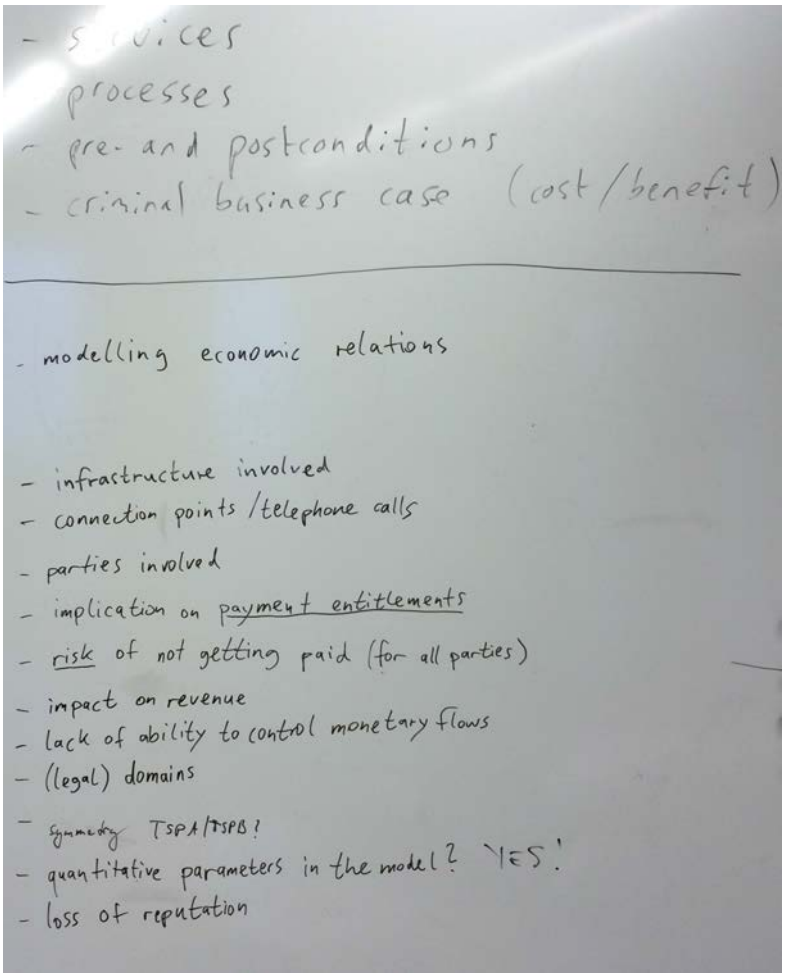

Figure A.1.: Telco case entity issues

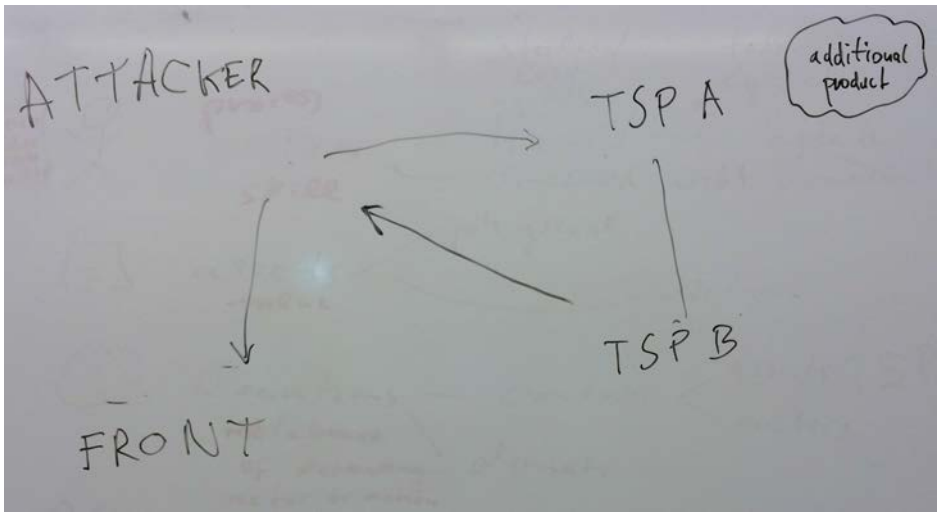

Figure A.2.: Telco case scenario 1 actor relations

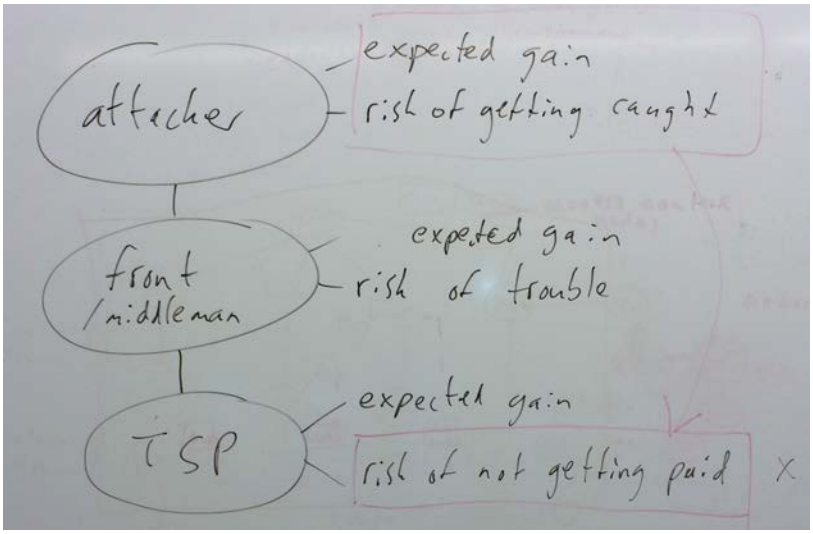

Figure A.3.: Telco case scenario 1 actors' expectation and risks

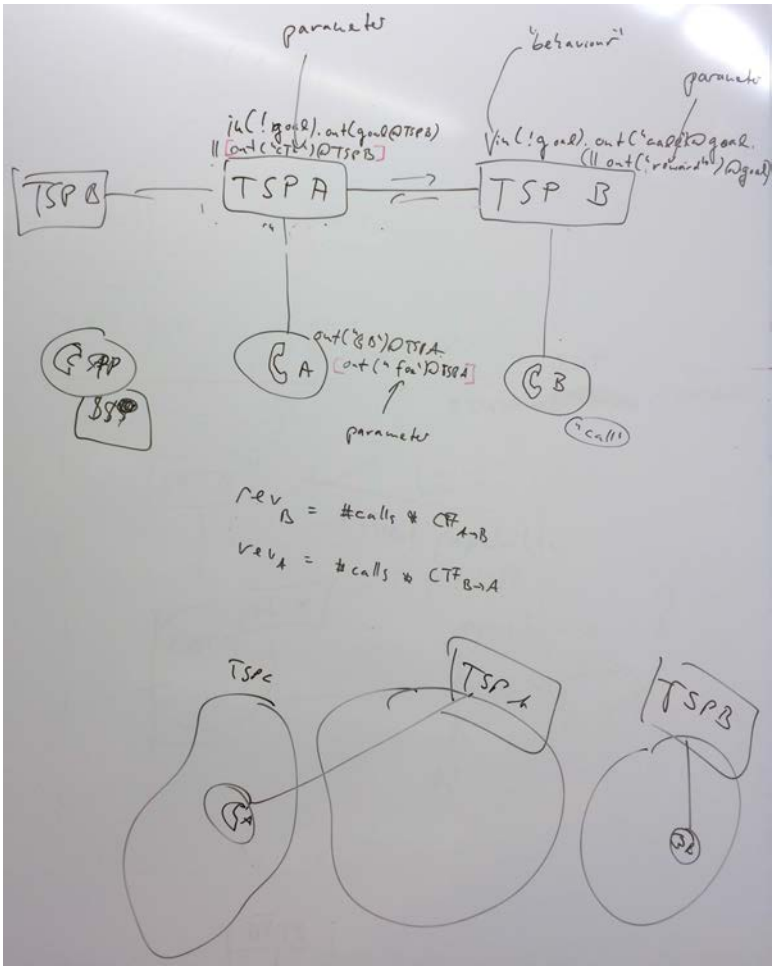

Figure A.4.: Telco case scenario 1 modeled using the TRE$_S$PASS model

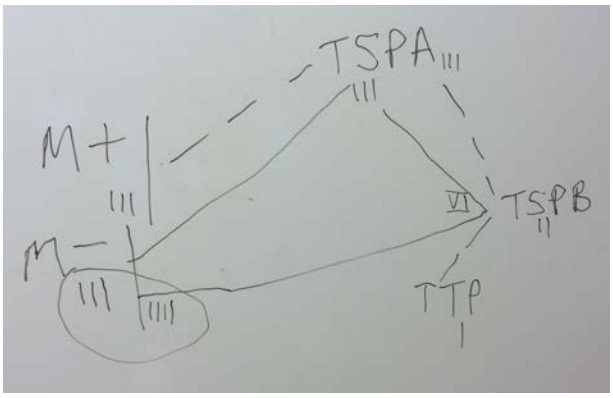

Figure A.5.: Telco case scenario 1 money flow

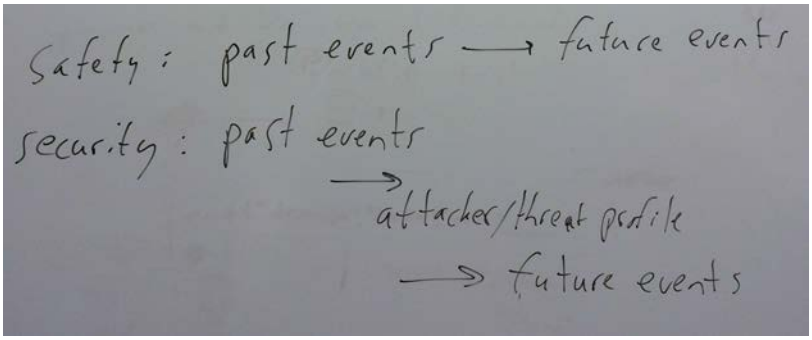

Figure A.6.: Distinguishing safety and security based on past and future events

B. Coordination models

Because e3value models do not include any process information, sometimes it is necessary to create an activity diagram or some other kind of coordination model in order to fully describe the scenario.

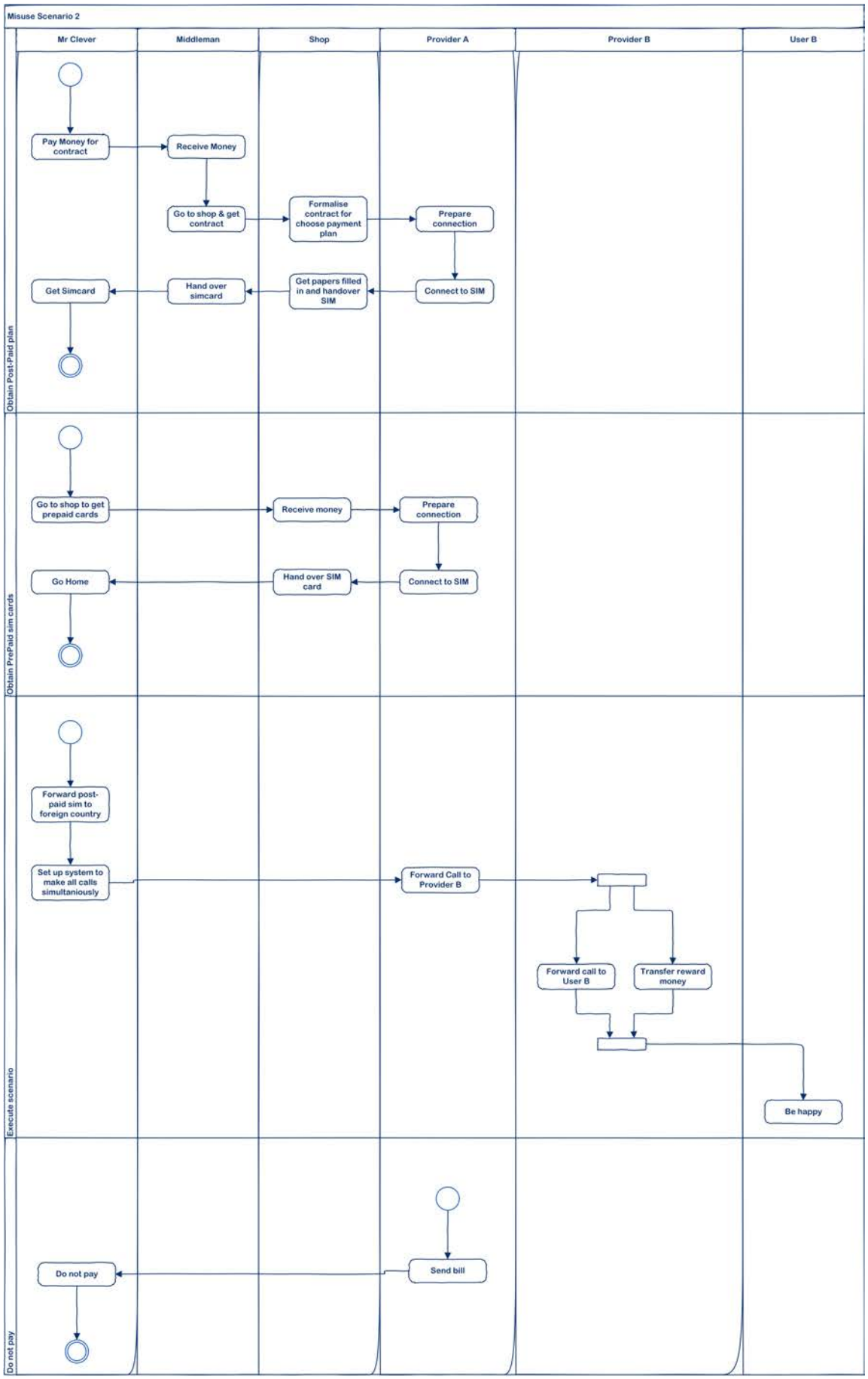

Figure B.1.: Coordination model of scenario 2