Modelling telecom fraud with $e^3$value

Dan Ionita  
SCS Group, University of Twente

Sebastiaan Koenen  
University of Twente

Roel Wieringa  
SCS Group, University of Twente

30th August 2014
## Contents

1 Introduction ................................. 4  
   1.1 Background ............................... 4  
       1.1.1 Telecommunication services ............ 4  
       1.1.2 e3value ............................. 5  
   1.2 Additional conventions .................. 7  

2 Scenarios and models ...................... 8  
   2.1 Base Case ............................... 8  
       2.1.1 e3value model ....................... 8  
   2.2 Scenario 1 - Flat-rate misuse ............ 10  
       2.2.1 e3value model ....................... 10  
   2.3 Scenario 2 - False pretence to pay ......... 12  
       2.3.1 e3value models ..................... 12  
   2.4 Scenario 3 - Intercepting e-Payments ...... 14  
       2.4.1 e3value models ..................... 14  
   2.5 Scenario 4 - Using someone else’s credit .. 18  
       2.5.1 e3value models ..................... 18  

3 Observations & Discussion ................... 20  
   3.1 Observations on model creation .......... 20  
   3.2 Limitations .............................. 20  
   3.3 Applicability ............................ 21  
   3.4 Future Work .............................. 22  

4 Conclusions ................................ 23  

A Coordination models ...................... 24
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Example and legend of an e3value model</td>
<td>6</td>
</tr>
<tr>
<td>1.2</td>
<td>Newly introduced e3value transaction types</td>
<td>7</td>
</tr>
<tr>
<td>2.1</td>
<td>Base case - e3value model</td>
<td>9</td>
</tr>
<tr>
<td>2.2</td>
<td>Scenario 1</td>
<td>10</td>
</tr>
<tr>
<td>2.3</td>
<td>e3value models for Scenario 1</td>
<td>11</td>
</tr>
<tr>
<td>2.4</td>
<td>Profitability graphs of Scenario 1</td>
<td>12</td>
</tr>
<tr>
<td>2.5</td>
<td>Scenario 2</td>
<td>13</td>
</tr>
<tr>
<td>2.6</td>
<td>e3value models of Scenario 2</td>
<td>15</td>
</tr>
<tr>
<td>2.7</td>
<td>Provider A’s profitability graphs for Scenario 2</td>
<td>16</td>
</tr>
<tr>
<td>2.8</td>
<td>Mr. Clever’s profitability graph for Scenario 2 (Mr. Clever view)</td>
<td>16</td>
</tr>
<tr>
<td>2.9</td>
<td>e3value models of Scenario 3</td>
<td>17</td>
</tr>
<tr>
<td>2.10</td>
<td>e3value models for Scenario 4</td>
<td>19</td>
</tr>
<tr>
<td>A.1</td>
<td>Coordination model of scenario 2</td>
<td>25</td>
</tr>
</tbody>
</table>
List of Tables

1.1 Values used for payment plans ..................................... 5
Chapter 1

Introduction

Telecommunication services are complex product packages that rely on a large and complex technical infrastructure. However, fraudulent use of such telecommunication services rarely exploits hardware vulnerabilities. Instead, most common exploits operate at a business level, capitalizing on the unexpected interaction between various product packages from multiple providers. 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 1.1.2) was selected, generic (non-misuse) business models were created and four misuse scenarios were modelled. This report showcases the models, discusses strengths and limitations encountered during modelling and draws conclusions with regard to the applicability, usability and utility of e3value models in modelling (Telecom) fraud as well as more generally in Risk Assessment.

1.1 Background

1.1.1 Telecommunication services

Telecommunications Service Providers (TSPs) commonly operate in highly competitive and dynamic markets, consisting of constellations of actors with conflicting (financial) interests. Thus, new and increasingly complex products and services are being rushed to market, leaving little time to assess potential risks. This provides fertile ground for unforeseen fraud or misuse. Most telecommunications products and services rely on a very complex underlying network architecture. This is due to a multitude of different interconnected networks, service providers and network operators. However, telecom misuse or fraud scenarios are largely independent of the underlying technical infrastructure. 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 this research is in its early stages, to ease the modelling effort, a set of idealizing assumptions with regard to the telecommunication services market are used throughout this research:

A **contractual period** of one month is assumed and used in the models.

**Payment plans** taken into consideration in this research are: Pre-paid (SIM with credit), Post-paid (SIM with subscription) and Flat-rate (SIM with unlimited calling). For each, realistic
<table>
<thead>
<tr>
<th></th>
<th>Prepaid</th>
<th>Postpaid</th>
<th>Flatrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial payment</td>
<td>5.00€</td>
<td>0.00€</td>
<td>0.00€</td>
</tr>
<tr>
<td>Monthly payment</td>
<td>0.00€</td>
<td>10.00€</td>
<td>37.50€</td>
</tr>
<tr>
<td>Cost per minute</td>
<td>0.03€</td>
<td>0.10€</td>
<td>0.00€</td>
</tr>
<tr>
<td>Interconnection fee</td>
<td>0.07€</td>
<td>0.07€</td>
<td>0.07€</td>
</tr>
<tr>
<td>Minutes included</td>
<td>334</td>
<td>-</td>
<td>∞</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>welcoming bonus.</td>
<td>until fair use</td>
<td></td>
</tr>
</tbody>
</table>

|                          |          |          |
|                         |          |          |

costs were pre-determined based on products currently available in the Dutch Telecommunications market in 2014. These costs are listed in Table 1.1.

**The bubble assumption** meaning that for each scenarios and model, only the selected sub-set of payment plans (which are known to allow for the misuse to take place) are taken into account.

**The behaviour of users** is flattened and averages are used to estimate the calling patterns of different types of users. For each model we consider at most two types of users: malicious and non-malicious.

### 1.1.2 e3value

The e3value modeling language was first introduced by Gordjin [4] 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 modeling concepts for showing which parties exchange things of economic value with whom, and expect what in return.” [5]. Figure 1.1 shows the building blocks of e3value and a simple example, showing the commercial relationships between the publishers of a number of newspaper tiles, their advertisers and and their readers. The main building blocks available in the e3value toolkit, as depicted in Figure 1.1, 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.

Looking at Figure 1.1, we observe that Readers have a need ("Read newspaper"). What the model then shows is that for each occurrence of this need (each Reader that decides he wants to read a newspaper), 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 Advertiser in exchange 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 responsible 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 Advertisers.

Occurrence 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 different 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 occurrences 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 occurrence rates of the same need, we are able to generate various profitability graphs, such as the one shown in Figure 2.4a.

However, it is important to remember that the order is which transactions occur along a depen-
dency 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.

1.2 Additional conventions

While creating value models of the misuse 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 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.

![Modelling conventions needed for this project](image)

**Figure 1.2:** Newly introduced e3value transaction types
Chapter 2

Scenarios and models

As a first step, a generic (non-malicious) scenario was created which shows the various payment plans commonly available to customers of Telecom Service Providers: 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 telecom provider (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. 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 provider 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.

2.1 Base Case

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

2.1.1 e3value model

The resulting e3value model is shown in Figure 2.1. 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 occur are deducted from the user’s account immediately. Most of the time this is done through some kind of crediting system.

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 2.1, provider 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 (Provider A).

In the bottom of the figure we position the receivers of the calls that the customers of Provider 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 (Provider 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.
2.2 Scenario 1 - Flat-rate misuse

Mr. Clever (a fraudster) has at least one fixed, mobile or virtual IP connection points with Carrier A which are billet either as flatrate or in tariff schemes which include capacious minute budgets. In addition, Mr. Clever has (multiple) fixed, mobile or virtual IP connection points with Carrier B, which provides bonuses to their customers when they receive calls. The bonus acts as an incentive for Mr. Clever to generate as much incoming traffic as possible to the B network, leading to an abuse of his contract with provider A.

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

2.2.1 e3value model

The telecom provider expects regular usage of the plan. His perspective of the business model is captured in Figure 2.3a. User A3 has flat rate contract with Provider A. User B2 has a contract with a different provider (Provider B). As Provider A is not expecting any deviant, there is no problem in User A3 calling User B2. Just an ordinary call. The expected profit of Provider A can be seen in Figure 2.4a.

However, Mr. Clever, the fraudster, has a different plan (Figure 2.3b). In his model user A3 and B2 are the same person (or at least working together). A clause unknown to provider A in User A’s contract with Provider B is introduced. User A now gets 0,055€ per incoming minute as a bonus for generating traffic. Provider B can afford to pay this bonus because of the interconnection fee of 0.07€ per minute it receives from Provider A.

This puts User A (a.k.a. Mr. Clever) in a potentially profitable position. Of course, in order to get to this profit, Mr. Clever needs to make calls for less than 0,055€ per minute. This can be achieved because of the flat rate plan. Actually, the more minutes are used, the lower the cost per minute. The expected gain of Mr. Clever can be seen in Figure 2.4b.
Figure 2.3: e3value models for Scenario 1
2.3 Scenario 2 - False pretence to pay

The second scenario has some similarities to the previous scenario, but involves an amplified attack using re-directed calls. Mr. Clever (a fraudster) obtains a large 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 Carrier A using forged or stolen identity and banking credentials. This is most easily achieved by hiring 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 100 €). The middle-man’s contract will rack up enormous charges but he never pay the bill. 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.

Mr. Clever activates call forwarding on the postpaid mobile connection and sets it up so as to redirect all calls to a (foreign) number on Carrier B’s network. Mr. Clever again has a contract with Provider B and again gets a bonus fee for every incoming minute. He then makes the highest number of possible parallel calls to that postpaid number using the prepaid SIM cards. This can be done for low costs as they are with the same provider. All these calls will be diverted to Carrier B and this forwarding will be charged on the postpaid account. For each received call on the foreign number, Mr. Clever is entitled to a bonus from Provider B.

The fraud detection system (FDS) of Carrier A will eventually detect a violation of the Fair Use Policy on the postpaid mobile connection contract and disconnect it within the response time. However, Mr. Clever will never pay the postpaid’s outstanding bill. Finally, Carrier B passes the received call termination fees in parts on to Mr. Clever, thereby providing a payout per minute for incoming calls.

2.3.1 e3value models

Figure 2.6a shows the perspective of Provider 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, a different user (User MM) has a postpaid
(a) False pretense of being willing and able to pay.

(b) Money flow.

Figure 2.5: Scenario 2
plan with the same provider.

In Figure 2.6b 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 Provider 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 intended interaction between the two contracts. The expected financial result of Mr. Clever, for various amounts of pre-paid SIMs is shown in Figure 2.8. 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 Provider A would face if User A is acting maliciously is shown in Figure 2.7b. If Mr. Clever was only to use 20 SIM cards these losses might amount to over 5000€ for one month. This is significantly different than the expected outcome of Figure 2.7a. Of course, the income gained from non-malicious users should also be considered, as the provider might still make a profit if only a small percentage of users acts maliciously.

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 A (FigureA.1)

The expected financial result of Provider A (per individual user) vs. the non-ideal financial result of Provider A (individual user) can be seen in Figure 2.7. Figure 2.7a also shows how this loss scales with the number of SIMs used by the fraudster.

2.4 Scenario 3 - Intercepting e-Payments

Compared to the previous scenarios, the upcoming scenarios are rather technical. This scenario involves the use of mobile wallets. “The mobile wallet is a new application of mobile payment that has functionality to supplant a conventional wallet and more. A mobile wallet is a much-advanced versatile application that includes elements of mobile transactions, as well as other items one may find in a wallet, such as membership cards, loyalty cards and travel cards.” [14]. These mobile wallets offer a new opportunity for fraud.

For the fraud case we examined, the payment functionality of the wallets is most important. When some user pays with his mobile wallet, the system sends a message to the service provider. This provider in its turn orders the transfer of the money from the user’s bank account to the account of the shop owner.

Fraud with this form of payment can be performed in several ways. For this scenario, a man-in-the-middle attack was used. This means the Internet packages containing the payment order are intercepted and tampered with. Here Mr. Clever has two options: changing the destination or change the destination and the amount. For this scenario the first was chosen. As divergent numbers are easier detected by the user, it was chosen to change the target account into Mr. Clever’s. For the execution of this attack, several techniques are available. For this research however, the specific technique is not important.

2.4.1 e3value models

In order to add quantitative information to the model, additional data is required. As mobile wallets are a new and upcoming payment method, not a lot of data is available about this. To
Figure 2.6: e3value models of Scenario 2
Figure 2.7: Provider A’s profitability graphs for Scenario 2

Figure 2.8: Mr. Clever’s profitability graph for Scenario 2 (Mr. Clever view)
work around this, we use available data about debit card payments (by PIN). This is currently a very popular payment method in the Netherlands. In 2013 2,660 billion transactions [3] were completed with an average value of €34,08. This combined with the fact that the amount of transaction under €10,00 is rising [1] shows the growing importance of digital payment. This growth is stimulated by businesses. For them, payment by PIN is cheaper than payment in cash[2]. The average cash payment costs 24 cent as a PIN payment costs 21 cent. From these costs a small part is a service fee to the provider. Based on data from ING bank [8] this fee is set at 5,2 cents per transaction. Based on these data and the above established base figure, the model were created.

Figure 2.9: e3value models of Scenario 3
2.5 Scenario 4 - Using someone else’s credit

This scenario is about technical PBX\(^1\) exploits. Although not many people know about these attacks, they are just as likely to occur as an attack on the data network[16]. There are several ways to attack a PBX. As Kuhn [11] describes, the most vulnerable is the remote access feature. Through this feature, for example, Mr. Clever can create a special mailbox which redirects him to a phone number of his choice (probably generating a bonus fee). Another option would be to get hold of a telephone within the company and start calling his number from there [13].

2.5.1 e3value models

Again a little extra information was needed to create the models. Firstly the costs of directing calls through a PBX was needed. This information was acquired from KPN [10]. Here it was found that an average call through a PBX costs 0,06 € per minute.

A new assumption was also made. It was assumed that the interconnection fee on landlines is lower than on mobile lines. This is a reasonable assumption, as otherwise KPN would not be able to make profit. Therefore the interconnection fee was set at 0,035 € per minute.

In figure 2.10a the business case as intended by the telecommunication services provider (Provider A) is modelled. As described above, company A is in the possession of a PBX system. This is used to make call through provider A and B to User B. In this model nothing extraordinary is occurring.

In figure 2.10b, the fraudster’s business case is modelled. By hacking into the PBX, he creates an opportunity for himself to make unauthorized calls. This can be done through the remote access of the PBX or physical access to one of the phones in the company. However, the technical means by which this is achieved is not captured in the e3value model. Through the PBX Mr. Clever will call a number of his choice. This number awards him (or a collaborator) a bonus fee. As Mr. Clever has no running costs for this scenario (except for the fixed costs of hacking into the PBX), his profit will be 5,5 cents per called minute. This scenario can be executed some time before it is detected, so it could become fairly profitable.

---

\(^1\)A private branch exchange (PBX) is a telephone exchange or switching system that serves a private organization and performs concentration of central office lines or trunks and provides intercommunication between a large number of telephone stations in the organization” [18]
Figure 2.10: e3value models for Scenario 4
Chapter 3

Observations & Discussion

3.1 Observations on model creation

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 provider as this behaviour deviates significantly from the provider’s execrations 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.

3.2 Limitations

Based on the e3value models, the profit or loss for both the telecom provider 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 telecom provider was obsolete. Assuming the modelling is undertaken by the provider 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 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.

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 run 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 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 the Telecommunication Services sector, and especially for the first two scenarios described in this document, this makes them ideal: information on the technical infrastructure is unobtainable, 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 more technical scenarios, 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 research, as indicated in Section 3.4. Furthermore, it now becomes crucial to find ways by which this variety of models can work together in an integrated work-flow. This is also briefly discussed in Section 3.4.
3.4 Future Work

This document only presents the results and observations of the first attempt at using e3value models as an alternative to more traditional architecture models commonly used in Risk Assessment to overcome the obstacles encountered especially in the Telecommunication Services fraud. 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 into existing Risk Assessment methodologies and frameworks. It is already obvious that they do not contain sufficient information to allow for the generation of attack vectors. Furthermore, since transformation to or generation of any sort of architecture or coordination model from an e3value model is not feasible [5], new ways have to be devised to allow exploiting the information available in these models such that it can be used in a Risk Assessment workflow.

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 [15, 9, 6] and [17, 12, 7], 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.

Finally, the current tool support is not intended for the type of models needed to describe fraud. The tool and computation engine need to at least support the supplementary conventions described in Section 1.2. Furthermore, the tool only generates static spreadsheets showing the financial results. All the graphs shown in this document were created manually by running the tool multiple times with variations in one parameter and extrapolating a function that could be used to plot the graphs. In the future, this should be supported natively by the tool, as graphs showing the variation of profit based on a parameter are much more revealing than single results.
Chapter 4

Conclusions

Overall, we have observed that e3value models successfully captured the economic aspects of the misuse scenarios modelled. Furthermore, they were somewhat easier to create as less knowledge about the technical infrastructure was needed and the building blocks and syntax are simpler. They 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, the e3value models will not be sufficient. In the latter two scenarios, which involve hacking of a TSP’s or TSP customer’s infrastructure, critical information about the attack is missing. 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, 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.
Appendix A

Coordination models

Because c3value 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 A.1: Coordination model of scenario 2
Bibliography


[8] ING.


[10] KPN.


[16] SMARTVOX.
