Automated identification and prioritization of business risks in e-service networks

Dan Ionita[1], Roel J. Wieringa[1], and Jaap Gordijn[2]

[1] University of Twente - Services, Cybersecurity and Safety group, Drienerlolaan 5, 7522 NB, Enschede, The Netherlands
{d.ionita,r.j.wieringa}@utwente.nl
http://scs.ewi.utwente.nl/

[2] Vrije Universiteit Amsterdam, De Boelelaan 1105, 1081 HV Amsterdam, Netherlands
j.gordijn@cs.vu.nl
http://e3value.few.vu.nl/

Abstract. Modern e-service providers rely on service innovation to stay relevant. Once a new service package is designed, implementation-specific aspects such as value (co-)creation and cost/benefit analysis are investigated. However, due to time-to-market or competitive advantage constraints, innovative services are rarely assessed for potential risks of fraud before they are put out on the market. But these risks may result in loss of economic value for actors involved in the e-service's provision.
Our *e*^{3}*fraud* approach automatically generates and prioritizes undesireable scenarios from a business value model of the e-service, thereby drastically reducing the time needed to conduct an assessment. We provide examples from telecom service provision to motivate and illustrate the utility of the tool.

Key words: e-services, value models, risk assessment, fraud

1 Introduction

Many services are *commercial* services. That is, they are of economic value to someone, and are paid for. As a result, end users and enterprises may be tempted to commit fraud or abuse, which we refer to as non-ideal behaviour. Such non-ideal behavior of actors involved in the acquisition or consumption of the service can lead to undesirable losses for the provider or undeserved gains for other actors. Examples include but are not limited to misusing the service, bypassing payments and exploiting unintended interactions between services. For example, in the field of telecom service provision, "simboxing" involves acquiring telephone services from multiple providers and setting up a composite service that disguises international calls as local traffic, thereby undercutting termination fees [1].

The problem is exacerbated because many services are in fact electronic services, which are provisioned via the Internet or other digital means [2]. These electronic services are characterized by short time-to-market (typically a few

months). But these e-services are provisioned over complex networks, that increases the opportunity for malicious actors to commit fraud or otherwise misuse e-services [3]. Risk assessment thus becomes more complex, and this creates a tension with the desire of marketeers to put out innovative e-services fast. Thus, there is a need to speed up and enhance the capability of e-service risk assessment.

Service innovation commonly consists of three phases: Service exploration, where potential new or improved services are identified; Service Engineering, where one or more of the options are explored in detail; and Service Management, which deals with implementation and continuity [4]. The Service Engineering phase carries particular importance, as errors introduced in the early phases of service design can have significant (financial) consequences later on [5, 6]. E-service risk assessment should therefore be done in the service engineering stage. This requires quantifying the cost of misuse and designing prevention or detection mechanisms, which in turn requires projections, usage estimates and financial computations [7]. Doing this in a way that does not unduly slow down service innovation requires efficient tool support.

Business risks for a provider include fraudulent violations of contracts by clients, violations of agreements or terms of service, as well as the creation, by clients, of false expectations with the provider with regard to usage. We define **fraud** as the intentional misrepresentation by a client of his or her intentions, in order to acquire something of value from a provider. Fraud may be legal or illegal. We call the actor performing a fraud a **fraudster.** In our assessment of fraud risk we sidestep the issue of legality but focus on the potential loss for the provider and potential gain for the fraudster. In other words, we focus on what is observable for the provider (his loss) and on what can be estimated about the fraudster, given a business model (his potential gain). The potential loss is the negative impact that the risk can have on the provider, and the potential gain for the fraudster indicates the likelihood that the fraud will be committed.

Previously, we introduced e^3fraud as a model-based approach to assessing business risks in e-service networks [8]. In that paper, we introduced three basic fraud operations, namely not paying for a delivered service, performing a hidden value transfer, and colluding with another actor; and we introduced different ways to estimate loss for a service provider and profit for a fraudster. Non-payment breaks transactional reciprocity (and causes loss) [9], hidden transfers can encourage misuse (by providing hidden gains) [10] and collusion allows exploiting unintended interactions between atomic services [11]. Our goal in this paper is to scale up these techniques to non-trivial scenarios by *automatically* generating fraud scenarios from a business value model. We will see that for realistic business models, the sheer number of possible variations is staggering, so the ability to filter, rank and group risks so as to zoom in on the most risky scenarios, becomes critical. With this paper, we aim to provide scalable tool support for generating, quantifying and ranking business risks directly from a business model of the given service.

Our approach to fraud risk assessment is constructive in the sense that we analyze the architecture of a business model, in particular a business model represented in e^3value , to construct possible mechanisms to commit fraud. This distinguishes it from statistical approaches to assess fraud risk [12], which use patterns of past client behavior to assess fraud risks in new business models. Since the new business model has by definition not contributed to the statistical data on which this assessment is based, statistics-based fraud assessment leaves one with unknown and un-estimated risks. Therefor, our approach is able to discover fraud scenarios a priori, while statistical models identify fraud a priori.

e^3fraud is based on the e^3value method for representing business models, and allows the generation of possible fraud mechanisms in new business models. The e^3fraud tool (available at: `https://github.com/danionita/e3fraud`) can automatically generate misuse scenarios based on configurable heuristics, such as collusion, non-payment and hidden payments. Furthermore, it can group and rank such scenarios on various criteria, such as loss to a service provider or profit to a fraudster. Finally, it can help visualize the financial results across a range of projected usage levels. We illustrate the tool using examples from telecom service provision.

The paper is structured as follows: Section 2 introduces the underlying e^3value language, the e^3fraud extension, and the new e^3fraud tool. Section 3 describes the application of the approach to a telecom service and showcases the results provided by the tool. Finally, Section 4 draws some conclusions with regard to the approach, its applicability and future development.

2 The e^3fraud methodology and tool

2.1 Starting point: e^3value

Value co-creation modeling is aimed at showing that a given business model is profitable for all (or most) of the parties involved in its provision and consumption. One established method for building value models and doing profitability computations is e^3value [13]. An e^3value model describing a flat-rate telephony service is shown in Figure 1. A flat rate, also referred to as a flat fee or a linear rate, is a pricing structure that charges a single fixed fee for a service, regardless of usage. [14]

An e^3value model represents how actors exchange commercial services in an ideal world during a period of time called the **contract period.** For example, Figure 1 may represent the way actors exchange services during a period of one month. An e^3value model assumes that all actors trust each other and all transactions occur as specified. It consists of several basic elements:

Actors are profit-loss responsible entities, such as organizations, customers and intermediaries. In Figure 1, the “Provider A”, “Provider B”, “User A” and “User B” are actors.

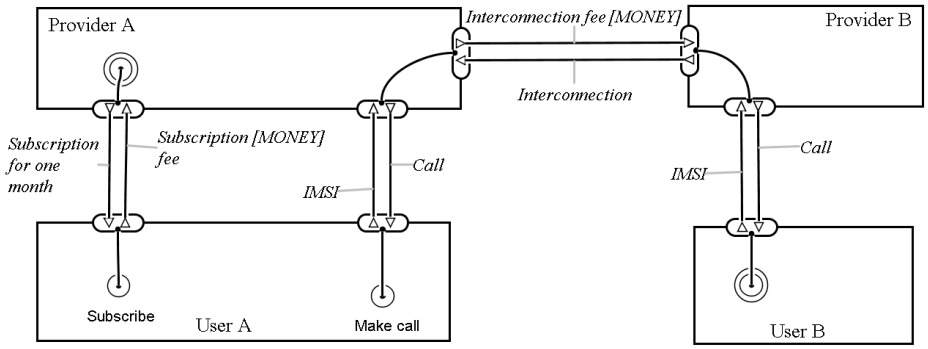

Fig. 1. e^3value model of flat-rate telephony service

Value objects are things of economic value, such as money, services, products, knowledge or experiences. In Figure 1 "Subscription for one month", "Subscription fee", ''IMSI" (International Mobile Subscriber Identity, used to identify the user of a cellular network and is a unique identification associated with all cellular networks. [15]), "Call", "Interconnection fee", "Interconnection" are all value objects.

Value transfers are transfers of value objects, such as a payment or the delivery of a service. In Figure 1, all the lines between two actors are value transfers.

Economic transactions are transactional groups of two or more (reciprocal) value transfers. In Figure 1, there are several such groups. E.g. "Subscription fee" in exchange for "Subscription for one month" and "IMSI" in exchange for "Call". Transactionality here means atomicity: if one transfer in a transaction occurs, all of them occur. Once we include the possibility of non-ideal worlds, as in e^3fraud , transactionality may be broken, because one actor may not deliver the value that is expected of it. In e^3value , however, transactionality is maintained

Dependency paths are chains of economic transactions. In Figure 1, there are two dependency paths: one for the subscription and one for the calling. Dependency paths do *not* represent processes [16]. They merely indicate that in the contract period, a consumer need triggers a certain combination of economic transactions, without saying when or how these transactions are performed. This is sufficient for doing profitability computations.

Consumer needs trigger a chain of economic transactions. In Figure 1, "Subscribe" and "Make call" are such needs.

Each value object has an associated monetary value (for each actor). Each consumer need has an associated occurrence rate (per contractual period). Both the monetary value and the expected occurrence rate need to be estimated by the user before any computations can be carried out. Together, these numbers can be used by the tool to estimate the financial result of each actor per contractual period.

e^3*value* is used to estimate whether a business model can be profitable under ideal circumstances of trusted actors. After the business model is fully understood, the next step is assess the risk(s) that not all actors behave as expected.

2.2 The *e*^{3}*fraud* methodology

In previous work [8] we've shown how an *e*^{3}*value* model can be extended to describe fraud. The resulting *e*^{3}*fraud* models differ from the original *e*^{3}*value* model in several ways, as described below (see figure 1).

- An *e*^{3}*fraud* model takes the point of view of one actor in the network, dubbed the **Target of Assessment** or ToA and marked with a thick border. This is needed to define the concept of hidden transactions, introduced below, and to assist with ranking the possible fraud models according to the potential loss for the ToA (further described in Section 2.3). In Figure 2, "Provider A" is the ToA.
- Value transfers may not take place and are marked using dashed lines. In Figure 2, the "Subscription Fee" transfer does not take place.
- Hidden transfers may occur between secondary actors, not involving the ToA and are marked using dotted lines. In Figure 2, a "Revenue Share" is being paid out by Provider B to User A for each call received. The ToA cannot directly observe these hidden transactions.
- Actors might collude, which means that they pool their budgets. In Figure 2, User A and User B are colluding. Collusion is usually kept hidden for the ToA.

Figure 2 shows that User A has a flat-fee subscription with provider A, and colludes with User B, who has a revenue-sharing subscription with provider B. An example of a revenue-sharing subscription is a subscription for an 0900 number, where the client is paid by the provider for being called. Provider B receives a large fee for providing access to an 0900 number, and shares some of this revenue with User B. The dotted line in figure 2 shows that this revenue-sharing payment is invisible to the ToA. By making the maximum number of calls to himself, User A+B can generate more income from the revenue-sharing subscription than the cost of the flat-fee contract. However, to increase profit, User A+B does not even pay the flat fee, as shown by the dashed line in figure 1.

This is just one possible sub-ideal model derived from the value model of a flat-rate show in Figure 1. The *e*^{3}*fraud* approach involves building several of these sub-ideal models, and comparing their financial outcomes to that of the ideal model in order to estimate the potential impact of each instance of fraud or misuse [8].

Manually creating these models and re-running the analysis is time-consuming, especially since the search space is potentially infinite. Furthermore, deciding which scenarios should be mitigated implies comparing a large number of models, and this cannot be done manually. In the following section, we describe our approach to delegate the time- and resource-intensive tasks of generation and ranking to a computer.

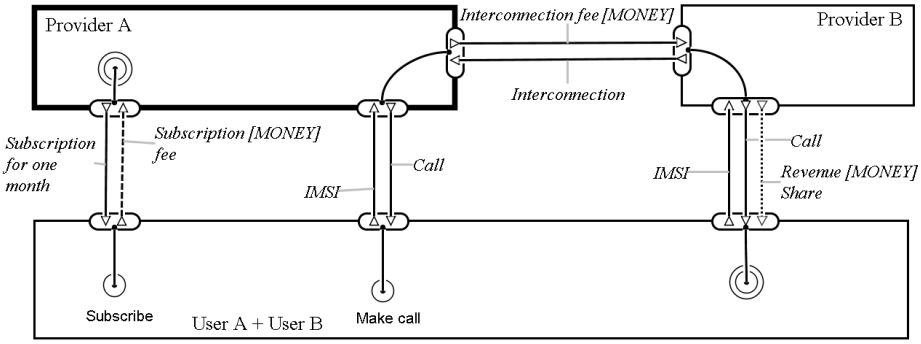

Fig. 2. *e*^{3}*fraud* model of flat-rate fraud

2.3 The *e*^{3}*fraud* tool

In this paper, we present a (tool-based) extension to the *e*^{3}*fraud* approach which allows the user to quickly and effectively generate, rank and compare possible sub-ideal variations of a given value model, based on several heuristics. The tool is open-source and publicly available at `https://github.com/danionita/e3fraud`. It performs three tasks:

1. Generating *e*^{3}*fraud* models, representing various fraud scenarios;
2. Ranking the generated *e*^{3}*fraud* models, so that the business model designer can zoom in on the most risky ones;
3. Computing and plotting the profit/loss of each actor across a given usage projection.

Generation Given a valid *e*^{3}*value* model, the tool generates all combinations of possible deviations: *hidden transactions, non-occurring transactions and collusions*. These patterns were previously found to be the building blocks of several telecom fraud scenarios [17]. Each valid combination is then instantiated as new sub-ideal model. A sub-ideal model may contain any number of hidden transactions and non-occurring transactions but only one collusion. The number of actors colluding is configurable.

Hidden transactions are generated in three steps.

– First identify pairs of transactioning secondary (non-ToA) actors.
– Then, for each such pair, the profit/loss resulting from the dependency path of which this transaction is part, is computed for each actor.
– Finally, for the actor(s) with a positive result, a new outgoing transaction is added: this transaction takes a value of one third and two thirds of the positive result, respectively. The reasoning behind this is that if an Actor makes some profit on a dependency path, he might be be willing to pass on 1/3 or even 2/3 of that value to another actor, B, if that would motivate B to generate more traffic. This models an established practice in the services industry called Revenue Sharing [18].

The generation of hidden transactions is thus bound by the number of actors and transactions in the ideal model.

Non-occurring transactions are created by invalidating individual monetary transfers (that is, transfers marked as type $MONEY$). The restriction to monetary transfers is to limit state space explosion, but this assumption could be dropped in the future. The user may indicate that certain $MONEY$ transfers will always occur by marking them as as type $MONEY\text{-}SECURE$. This can be either because they are initiated by the provider itself, because safeguards are in place or simply to reduce the search space of sub-ideal models. This will prevent these transfers from being invalidated by the generation engine. The generation of hidden transactions is thus bound by the number of monetary transfers in the ideal model.

Collusion takes place when two actors are acting as one: they pool their budgets and collectively bear all expenses and profit. By colluding, actors might deceive controls and invalidate expectations by appearing independent but in fact working together against the best interests of the provider. Therefore, only secondary actors (not the ToA) can collude. To generate collusions, pairs of secondary actors are merged into a single actor. The number of actors allowed to part of a colluding group is configurable. The generation of collusions is thus bound by the number of actors in the ideal model.

Ranking Depending on the complexity of the initial ideal model, hundreds of even thousands of models might be generated. Many of these might not be possible due to existing controls or might be unlikely because they are not profitable for any of the actors.

To aid with selection and prioritization of risks, the tool provides several ways of ranking and grouping the set of generated models, described below. The prioritization is always carried out from the perspective of a single actor (the Target of Assessment), as described below.

In terms of value creation, non-ideal behavior causes a disruption in the financial result of the actors involved. This means that a non-ideal scenario can (1) cause a loss for the service provider and (2) trigger an unexpected gain for one of its customers or users. As such, the software tool allows ranking based on Loss for the ToA, Gain for the secondary actors and Loss+Gain. Gain for a secondary actors is defined as the difference between the financial result of a that actor in the ideal case versus the sub-ideal case.

Ranking on Loss+Gain ranks risks on negative impact for the ToA (Loss) and profitability for the potential fraudster (Gain). This is similar to the classical definition of risk as Impact times Likelihood of an event, except that we do not use Likelihood of the fraud but Gain to the fraudster. We use Gain to estimate the attractiveness of a fraud to a potential fraudster. A fraud with a higher gain for the fraudster is more attractive to the fraudster, and therefore more likely, than a fraud with a lower gain.

Furthermore, to allow for"what-if" analyses and easier navigation through the long list of sub-ideal models, results can be grouped based on who is colluding

with who. Since each group is ranked independently, this allows investigating the most risky way each pair or group of actors can collude.

Visualization The ranked list of generated sub-ideal models is presented by the e^3fraud tool as a list of textual descriptions. If grouping was selected, the list is nested and collapsible. This facilitates the exploration of the state space. Additionally, the financial results of the ideal models and any of the sub-ideal modes can also be visualized as a 2D plot showing the profit/loss across a range of usage levels for the fraudster and for the ToA. The user may select which usage indicator (i.e. consumer need) to be represented on the X-axis, as well as its range. We provide a detailed illustration later in Figure 5. These representations can be understood by marketeers and product managers without having to learn e^3value or e^3fraud .

The results contain several useful pieces of information. Firstly, they show the loss for the ToA across the given occurrence range, as both a plot and an average. Loss is a direct indicator of the potential impact that each of the particular fraud risks can bring about. Secondly, the gain experienced by all other actors in the model is also shown as both a plot and an average. This gain can be used as a proxy for likelihood: the higher potential gain for some actor, the more likely it is that he will attempt that specific fraud scenario. Finally, the slope of all the plots are estimated, which gives an indication of how the loss and gain of the fraud scales with usage, outside the given range, and therefore how the impact and likelihood vary. Visualizing the result as a plot also allows for easy, visual identification of break-even points and thresholds.

3 Preliminary evaluation results

The approach has been applied to several telecom service packages known to be exploitable. In this section, we present one of these cases: call forwarding to other networks via post-paid subscription.

The (ideal) value model of this service is shown in Figure 3. Provider A is our target-of-assessment, i.e. the entity who is offering the service and conducting the assessment. User A is a customer of Provider A. In this case, he is using a pre-paid SIM card to make calls to some other customer of Provider A: User B. User B, in turn, has a post-paid subscription with Provider A. This subscription involved a fixed monthly payment, plus an incremental payment based on his usage. In this simple example, he does not initiate any calls and has set his device to forward all received calls to User C. User C is a customer of Provider B, and therefore User B will have to pay for the connection from his own Provider, A, to User C. Since Provider B is a separate commercial entity, we do not know his contractual structure nor his usage pattern, so we only model the fact that User C can receive calls.

A known fraud scenario (shown in Figure 4) for this case is as follows: User A initiates a very large number of calls to User B. The calls are usually charged at a preferential rate, as the two users are on the same network. User B, as

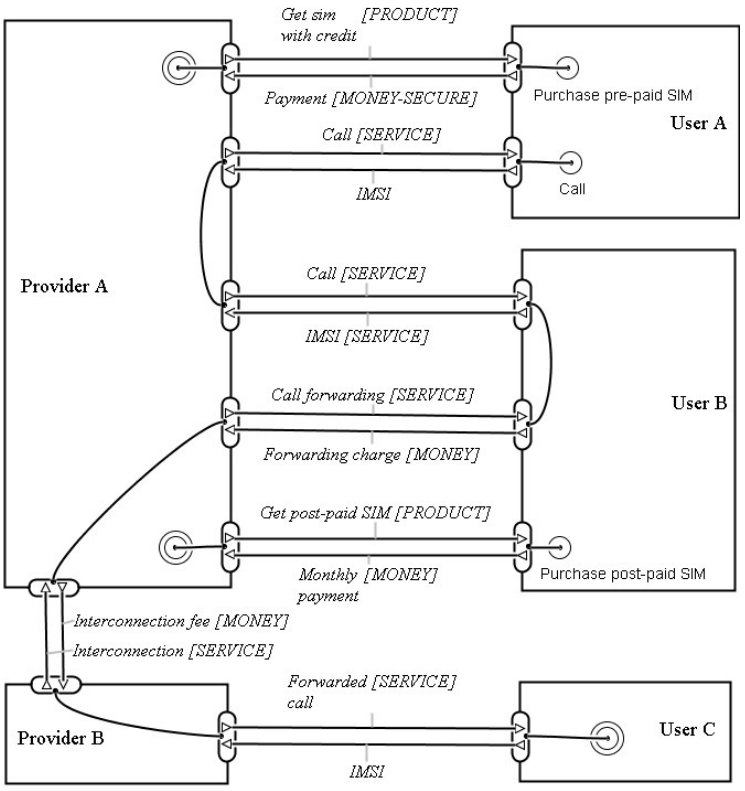

Fig. 3. Value model of call forwarding to other provider

the forwarding party will have to pay for the call outside the network. He will receive a very large bill at the end of the month, which he does not pay. In reality, User A commonly pays User B a small amount of money to start a post-paid subscription using fake credentials, so that User B cannot be traced by Provider A. Finally, User C, the end-recipient of the call would have a Revenue Sharing agreement with Provider B, by which he receives a pay-out for every call that comes through. This is common with 0900 numbers but also available with some "budget" subscriptions.

By running the model in Figure 3 through the e^3*fraud* tool using default settings, we obtain the fraud scenario described above and visualized in Figure 4 as the 7th highest ranked scenario. Figure 5 shows a screen-shot of the actual output. The left part of the screen describes the 7th highest ranked risk as:

Average of **-11.23** (instead of **25.82**) for Provider A due to:
Colluding actors "User A" and "User C"
Non-occurring exchange Forwarding charge
Non-occurring exchange Monthly Payment

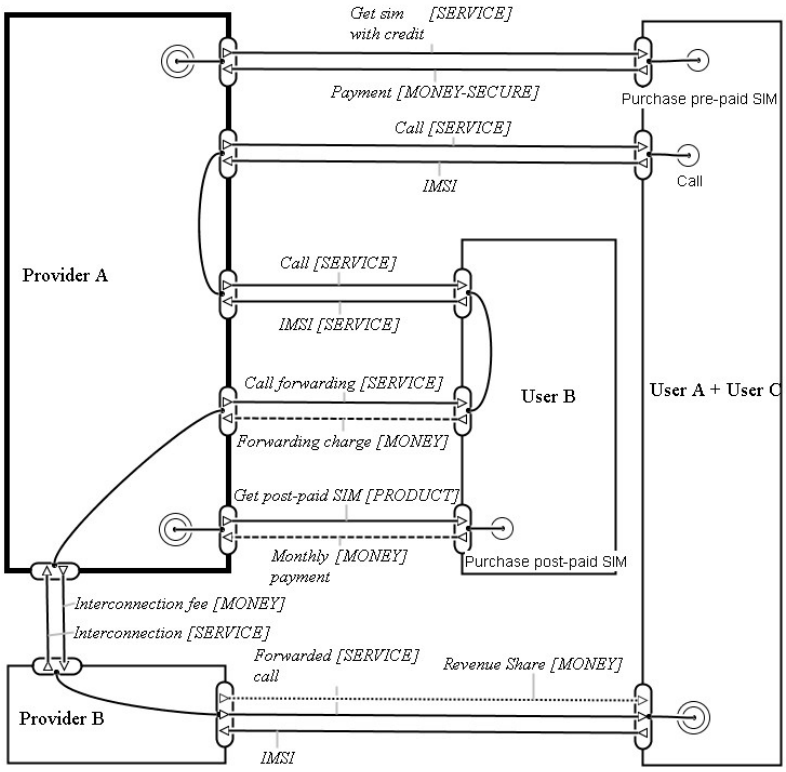

Fig. 4. e^3fraud model of fraudulent call forwarding to other provider

Hidden transfer of value 0.02 (out of 0.03) from "Provider B" to "User A + User C"

The value in brackets of 25.82 is the average profit for the ToA in the ideal case (i.e. the model provided as input to the tool). The assumption is that this value is what the ToA would have expected to obtain given its own estimates. However, in this scenario, the ToA will only obtain an average of -11.23 across the same occurrence rate. The reasons for this are also given by the tool: two actors (Actor A and Actors C) are colluding, User B will not pay his bill this month (consisting of a Monthly Payment and a Forwarding charge, and Provider B is passing two thirds of his revenue per call to the now colluding Users A and C. The tool uses the total incoming value per occurrence rate as a basis for this last estimation of 0.02 out of 0.03.

The right part of the screen shows the evolution of the risk with the number of (forwarded) calls per contractual period. The x-axis represents the number of calls by User A and the y-axis represents the corresponding profit and loss for the actors. The steepest upward line is "User A + User C" (the fraudsters). The next steepest upward line is "Provider B". The horizontal line is User B, and the downward line is Provider A (the ToA). The graph therefore shows that

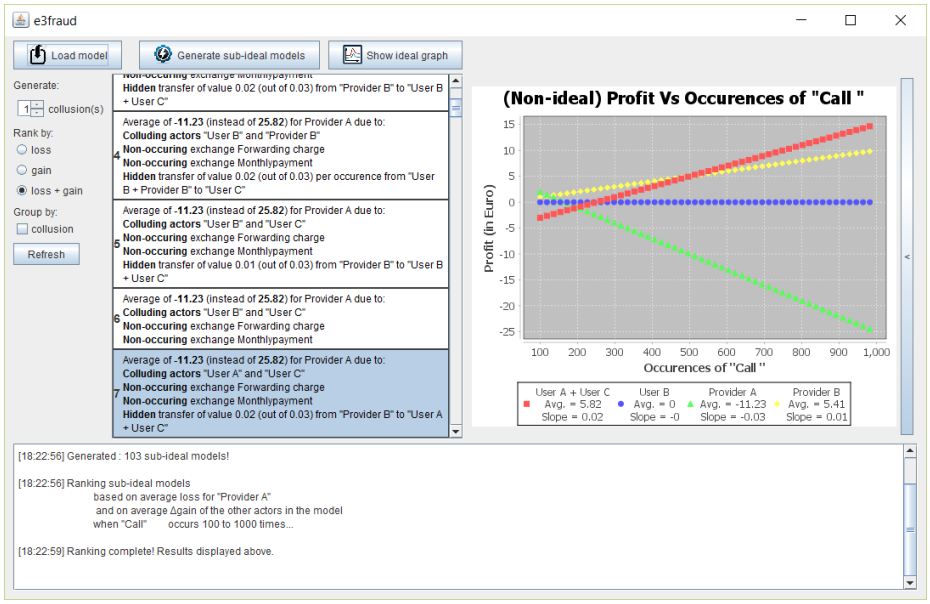

Fig. 5. Screen-shot of the e^3*fraud* tool's output for the value model in Figure 3.

this particular scenario allows the two colluding actors to obtain a sizable profit, that scales very well. It also shows that this would cause an unexpected loss for the provider, which gets significantly worse with the number of minutes called. Provider B maintains a positive financial result, and User B does not incur any loss or profit from participating in this scenario.

The higher ranked risks (numbers 1 to 6 in the list) trigger the same loss for the provider, but yield a higher profit for other groups of colluding actors at the detriment of other secondary actors, making them unrealistic. For instance, it makes no (financial) sense for Actor A to initiate the calls in the first place if he is in on the fraud. Furthermore, other highly ranked risks imply a User colluding with Provider B, thus also obtaining Provider B's legitimate interconnection income. While collusion between user and providers is not impossible, in this case it is extremely unlikely. Grouping the results per collusion would help in this case to eliminate unrealistic collusions from the analysis.

These results can help design fraud detection thresholds, identify transaction that require (further) procedural or technical controls or even trigger a re-design of the service in order to eliminate or mitigate business value risks [7].

4 Discussion and future work

This e^3*fraud* approach described in this paper provides a novel, constructive, semi-automated method for conducting quantitative risk assessments of value models. The approach relies on a small set of misuse patterns commonly seen in

telecom fraud, that so far has been sufficient to generate known fraud scenarios. Our results highlight the potential of automating the identification, quantification and ranking of business risks associated with one or more service offerings.

As noted earlier, telecom providers already have statistical means of estimating fraud [12]. But these means assume the future is like the past. Predictive models based on large data sets of past service deliveries do not necessarily indicate what the risks of new, innovative e-service provision arrangements are. *e*^{3}*fraud* provides a supplementary approach that analyzes the architecture of a service provisioning network and identifies risks that follow from the structure of the network, by actually constructing the fraud mechanisms. This allows marketeers and managers to identify the source of these risks and take preventive measures, before the risks materialize.

So far we have only found known fraud scenarios. Understandably, telecom providers are reluctant to disclose all of the fraud scenarios known to them, and so it will be very hard for us to know whether fraud scenarios generated by our tool were already known to them or not.

Weve shown feasibility in other cases [8]. However, more real-world cases are of course needed to confirm generalizability. To test whether we can find fraud scenarios not known to *us,* we will collect new business models and try to identify unexpected scenarios. To further test the generalizability of our ideas, we intend to analyze fraud in other kinds of e-services, outside the telecom sector. If this too results in the identification of unknown fraud possibilities, this would confirm the power of our basic fraud operations. Alternatively, we can use the new scenarios to distill a more complete set of fraud patterns and heuristics. Implementing them into the tool's generation and ranking modules in a customizable way would further the flexibility and applicability of the approach. For instance, it might be the case that in certain scenarios, higher gain does not necessarily imply higher likelihood. Therefor, it is worth exploring alternative heuristics in future research.

Finally, a larger search space also raises issues of resource exhaustion; care must be given to trimming the search space and streamlining code. One way of limiting the search space seems to be to differentiating between clients and providers. Then, only clients can be assumed to collude or attempt to bypass payments. Another way of managing the potentially very large lists of results is filtering. Therefore, one of the main topic for improvement in the future is integrating a filter functionality in the tool. Examples filters are: removing sub-ideal models that do not cause a loss, removing sub-ideal models that are not profitable for any of the actors and only showing the most profitable or costly sub-ideal model per collusion type. Furthermore, integrating a model editor into the tool might further increase its usability: firstly, users would need not go through the export/import process for every instance of a model and secondly, users would be able to visualize the fraud directly on the value model.

References

1. Reaves, B., Shernan, E., Bates, A., Carter, H., Traynor, P.: Boxed out: Blocking cellular interconnect bypass fraud at the network edge. In: 24th USENIX Security Symposium (USENIX Security 15). pp 833–848. Washington, D.C., USENIX Association (August 2015)
2. Mohan, K., Ramesh, B.: Ontology-based support for variability management in product and families. In: Proceedings of the 36th Annual Hawaii International Conference on System Sciences. pp 9–18 (Jan 2003)
3. Carbo, J., Garcia, J., Molina, J.: Trust and reputation in e-services: Concepts, models and applications. In: Lu, J., Zhang, G., Ruan, D. (eds.) E-Service Intelligence. Studies in Computational Intelligence, vol. 37, pp 327–345. Springer Berlin Heidelberg (2007)
4. Tan, Y.H., Hofman, W., Gordijn, J., Hulstijn, J.: A framework for the design of service systems. In: Service Systems Implementation. Service Science: Research and Innovations in the Service Economy, pp 51–74. Springer US (2011)
5. Soomro, I., Ahmed, N.: Towards security risk-oriented misuse cases. In: Rosa, M., Soffer, P. (eds.) Business Process Management Workshops. Lecture Notes in Business Information Processing, vol. 132, pp 689–700. Springer Berlin Heidelberg (2013)
6. Yu, E.S.K.: Models for supporting the redesign of organizational work. In: Proceedings of Conference on Organizational Computing Systems. COCS '95 pp 226–236, New York, NY, USA, ACM (1995)
7. Cahill, M., Lambert, D., Pinheiro, J., Sun, D.: Detecting fraud in the real world. Massive Computing , vol. 4, pp 911–929. Springer US (2002)
8. Ionita, D., Wieringa, R.J., Wolos, L., Gordijn, J., Pieters, W.: Using value models for business risk analysis in e-service networks. In: 8th IFIP WG 8.1. Working Conference on the Practice of Enterprise Modelling. Lecture Notes in Business Information Processing, vol. 235, pp 239–253. Berlin, Springer Verlag (November 2015)
9. Ruch, M., Sackmann, S.: In: Customer-specific transaction risk management in e-commerce. Lecture Notes in Business Information Processing, vol. 36, pp 68–79 Springer Berlin Heidelberg (2009)
10. L., D., J., M.: A game of clicks: Economic incentives to fight click fraud in ad networks. Performance Evaluation Review 41, pp 12–15 (2014)
11. Pieters, W., Banescu, S., Posea, S.: System abuse by service composition: Analysis and prevention. In: CESUN 2012: 3rd International Engineering Systems Symposium Delft University of Technology, The Netherlands, 18-20 June 2012. (2012)
12. Richard J. Bolton, D.J.H.: Statistical fraud detection: A review. Statistical Science 17(3), pp 235–249 (2002)
13. Gordijn, J., Akkermans, H.: Designing and evaluating e-business models. IEEE Intelligent Systems 16(4), pp 11–17 (July 2001)
14. Gerpott, T.J.: Biased choice of a mobile telephony tariff type: Exploring usage boundary perceptions as a cognitive cause in choosing between a use-based or a flat rate plan. Telematics and Informatics 26(2), pp 167–179 (2009)
15. Scourias, J.: Overview of the global system for mobile communications. Technical report (1995)
16. Gordijn, J., Akkermans, J., Vliet, J.V.: Business modelling is not process modelling. In: Conceptual Modeling for E-Business and the Web. Proceedings of the ER 2000 Workshops on Conceptual Modeling Approaches for E-Business and The World Wide Web, pp 40–51. Springer, Salt Lake City, Utah, USA (2000)

17. Ionita, D., Koenen, S.K., Wieringa, R.J.: Modelling telecom fraud with e3value. Technical Report TR-CTIT-14-11, Centre for Telematics and Information Technology, University of Twente, Enschede (October 2014)
18. Ross, S.: How does revenue sharing work in practice? Investopedia (2015), http://www.investopedia.com/ask/answers/010915/how-does-revenue-sharing-work-practice.asp [Online; accessed 12-December-2015].