Using Value Models for Business Risk Analysis in e-Service Networks

Dan Ionita, Roel J. Wieringa, Lars Wolos, Jaap Gordijn, Wolter Pieters

Using Value Models for Business Risk Analysis in e-Service Networks

Dan Ionita[1], Roel J. Wieringa[1], Lars Wolos[2], Jaap Gordijn[3], and Wolter Pieters[1,4]

[1] University of Twente, Drienerlolaan 5, 7522 NB Enschede, Netherlands,
{d.ionita,r.j.wieringa}@utwente.nl
[2] Goethe University Frankfurt, Frankfurt, Germany
lars.wolos@m-chair.de
[3] Vrije Universiteit Amsterdam, De Boelelaan 1105, 1081 HV Amsterdam, Netherlands
gordijn@cs.vu.nl
[4] TU Delft, Mekelweg 5, 2628 CC Delft, Netherlands
w.pieters@tudelft.nl

Abstract. Commercially provided electronic services commonly operate on top of a complex, highly-interconnected infrastructure, which provides a multitude of entry points for attackers. Providers of e-services also operate in dynamic, highly competitive markets, which provides fertile ground for fraud. Before a business idea to provide commercial e-services is implemented in practice, it should therefore be analysed on its fraud potential.

This analysis is a risk assessment process, in which risks are ordered on severity and the unacceptable ones are mitigated. Mitigations may consist of changes in the e-service network to reduce the attractiveness of fraud for the fraudster, or changes in coordination process steps or IT architecture elements to make fraud harder or better detectable.

We propose to use e^3value business value models for the identification and quantification of risks associated with e-service packages. This allows for impact estimation as well as understanding the attacker's business cases. We show how the e^3value ontology — with minimal extensions – can be used to analyse known telecommunication fraud scenarios. We also show how the approach can be used to quantify infrastructure risks. Based on the results, as well as feedback from practitioners, we discuss the scope and limits of generalizability of our approach.

Key words: e-services, fraud, risk, governance and control, value modelling

1 Introduction

e-Services, commercial services delivered electronically [12], are of vital and increasing importance to society. Examples are internet provision services, telephony services, email services, on-line delivery of music or other content, e-banking, on-line booking, etc. These services are delivered fully electronically, as

opposed to many other 'physical' services such as a haircut at a barber. In this paper we will use telephony services as running examples.

The delivery of e-services is done via an *Information and Communication Technology (ICT)* infrastructure. For instance, modern telephony connections are handled by a complex technical architecture and rely on several information systems, e.g. for billing or call management. Technical vulnerabilities in such infrastructures may cause great concern [2].

However, since e-services are commercial offerings, they have *commercial* vulnerabilities in addition to technical ones. For instance, it is possible to register a telephony subscription using the identity of someone else (e.g. by providing a false proof of identity in the subscription process), resulting in calling for free.

These problems are exacerbated in highly competitive e-service markets such as telecom and on-line content provision, where service providers struggle to increase their market share by pushing new, increasingly flexible service packages with low and sometimes even negative margins. In an effort to reduce time to market, service providers might not have the time or resources to fully assess the potential for loss of each new service package. However, due to the increasingly complex and inter-connected nature of e-service provision, these plans often contain loopholes which malicious customers might abuse in order to reduce their costs or even turn a profit. Traditional heavy-weight GRC[1] frameworks are therefore of little use to analyse fraud potential: their models are focused on the socio-technical layout while established methods are mostly concerned with confidentiality, integrity and availability issues and may take days or weeks to apply [7].

We propose e^3*fraud* for risk analysis in e-service networks. e^3*fraud* is based on the e^3*value* ontology [3] for exploring new e-business ideas. e^3*fraud* conceptualizes risks in a *model*-based way, using a business oriented terminology. This ensures that the approach is usable by IT-oriented stakeholders, while keeping business concerns in mind. We present examples of fraudulent behaviour in the telecom industry, and show how to analyse them using e^3*fraud*. Furthermore, we show how the approach could be used to model the commercial aspects of infrastructure risks.

Our methodology explicitly recognizes the notion of a *value constellation* [13]. Many e-services in fact are value constellations because they require multiple profit-loss responsible actors to collaborate in order to produce value for the customer. For example, in the telephone domain there is a caller, a callee, one or more telecommunication companies (e.g. for transit traffic), parties for billing and selling of prepaid cards, etc..

This paper is structured as follows: In Section 2 we summarize the steps taken to produce the results presented in this paper. In Section 3 we outline the e^3*fraud* approach to analyse *commercial* risks in networks of e-services using two cases provided by a telecommunication operator. In Section 4 we show how the e^3*fraud* approach could be used to quantify known *infrastructure* risks. Section 5 tackles some of the issues encountered by the authors.

[1] Governance, Risk and Compliance

2 Research Methodology

The approach undertaken follows the traditional Design Cycle [18]. Partners from the telecom industry put forth the need for an approach to conducting lightwieght risk analysis of new service packages before they hit the market and provided several fraud scenarios for analysis. Investigation of these scenarios revealed that they could be commonly described solely in terms of value exchanges amongst the actors.

Based on previous experience in creating value models and doing profitability analyses of a value constellation, we selected the e^3value framework as a starting point. The e^3value approach models a network of end users and enterprises who exchange things of economic value with each other. However, e^3value is designed for mutually beneficial value models. So we iteratively extended the e^3value ontology and toolkit so as to accommodate the scenarios in questions (see Section 3.3) and provide meaningful output (see Section 3.4), respectively.

The long term goal of this research is to facilitate automatic identification, modelling and analysis of business risks related to e-service provision by software tool support. In this paper, we present two real life case studies demonstrating our modelling conventions and analysis approach. Most of the results shown were produced using software tools: for the creation of the initial models, tool support is available (see `e3value.few.vu.nl`) and for running the analysis a custom Java extension was created.

For initial validation, we obtained feedback from a telecom provider about their perception of the potential usability and utility of our approach in practice, which we discuss in Section 5.1.

3 The e^3fraud Approach to Analysing Business Risks in Networks of e-Services

The e^3fraud approach takes as input an ideal business model and produces a set of sub-ideal business models. Each sub-ideal business model represents a business risk, for which graphs can be generated showing the loss/gain of each Risk.

The e^3fraud approach consists of three steps:

1. Construct the ideal business value model in e^3value, showing the e-service at hand in terms of expected economic value creation and distribution
2. Construct/generate one or more sub-ideal models ine^3fraud, showing possible fraud scenarios in terms of economic value
3. Analyse financial feasibility and financial impact of the fraud

Steps 1 and 2 are also proposed by Kartseva et al. [10]. However, where Kartseva et al continue with proposing solutions to possibilities to prevent committing a fraud, the e^3fraud analyses in step 3 the financial feasibility of the fraud for the fraudster, and the financial impact of the fraud on the ToA. In other words: the attack should be profitable for the attacker; otherwise the attack is not financially feasible. In addition, the attack should be costly for the

ToA; otherwise countermeasures are not financially feasible. This allows stakeholders to assess the severity of a fraud scenario represented by the sub-ideal model, and helps decision makers choose which scenarios need to be mitigated.

Furthermore, in Kartseva models [9], sub ideal model behaviour is represented by value transfers that do not occur (e.g. a customer not paying for a product), or occur wrongly (e.g. paying an insufficient amount of money). *e*^{3}*fraud* adds the notion of *hidden* transfers: fraudulent behaviour might involve value transfers that some (honest) parties do not expect or cannot observe, but of which they later experience the financial effects. This implies that an *e*^{3}*fraud* model now takes the *perspective* of an individual enterprise or customer.

Currently, as a proof of concept, sub-ideal models are constructed manually, but we plan to provide tool support for automatic generation and ranking of sub-ideal models.

3.1 Scenario Description

In this section we explain the *e*^{3}*fraud* approach by means of an easy to understand example, from the field of telecommunication/telephony.

A simple example of fraud in the telephony sector is Revenue Share Fraud (RSF), and involves setting up revenue sharing agreement with one provider, and a flat-rate (unlimited) subscription with another, and then calling yourself. This triggers the payment of interconnection fees from one provider to the other, thus resulting in a transfer of economic value between the providers. Depending on the scale of the operation and the detection capabilities of the provider, fraudsters could pull in up to several million dollars over a weekend [1]. We define Telecom misuse as the contracting or consumption of telecommunication services in a manner that is not in line with the service provider's expectations. Fraud is then any instance of misuse as previously defined with the explicit goal of obtaining financial rewards.

3.2 Construction of an Ideal Business Value Model

We develop first an ideal business value model. Such a model shows what actors transfer in terms of economic value if all actors behave *honestly*. We explain *e*^{3}*value* as we go along.

Figure 1 presents the ideal business value model for a flat-rate mobile phone subscription. The *e*^{3}*value* language supports the notion of *actors*. Actors are profit-and-loss responsible enterprises, non-profit organizations, or end-users. In this specific example, actors are telecommunication providers (provider A and B) and end users (user A and B).

The *e*^{3}*value* language also has the construct of *market segment*. A market segment groups actors that assign economic value to received or provided objects in the same way. For explanatory reasons, we do not use the notion of market segment yet.

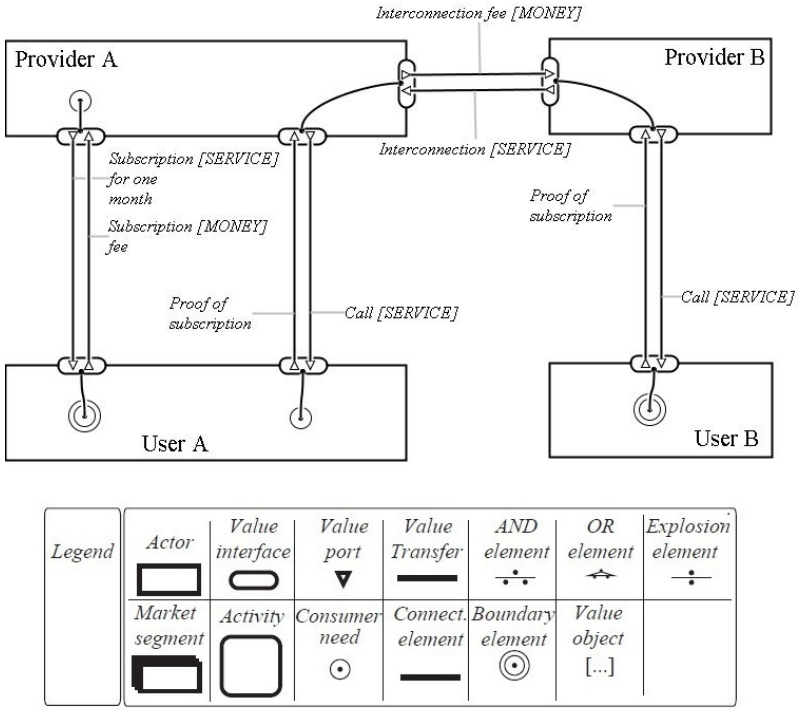


Fig. 1. Ideal model: User A calls user B

Actors exchange things of economic value with each other, called *value objects*, via *value transfers* (visualized as straight line *between* actors). Value objects are physical objects or outcomes of services that are experienced by at least one actor in the model as of economic value.

In Figure 1 user A obtains a monthly flat-rate subscription ("Subscription for one month") with Provider A and in return for this, the users pays Provider A an amount of money on a monthly basis ("Subscription fee"). The flat-rate subscription entitles the users to perform unlimited telephone calls to any other number. In return for presenting proof of this subscription to the provider, the provider delivers its service, which is a telephone call.

In many cases, the caller and the callee do not have a subscription with the same provider, but rather with two providers, in Figure 1 provider A and B. So, to create a telephone connection initiated by user A to user B, provider A has to interconnect with provider B, since provider B is the operator user B has a subscription with. In other words, provider B delivers an interconnection service to provider A, and this service of value to provider A, because otherwise provider A could not create telephone connection outside its own network.

User B has his own contractual agreement with Provider B. However, this ideal model is built from the perspective of Provider A for whom the structure

of this agreement is not know nor observable and thus not represented. The only transaction between User B and Provider B which Provider A can observe is the telephone call.

An *e*^{3}*value* model shows how actors do business which each other in a *contract period.* This is a period described by the contracts that describe the value transfers among actors shown in the diagram. An important property of an *e*^{3}*value* model is *economic reciprocity.* Figure 1 shows various *value interface*s, containing *value port*s, transferring value objects (see the legend). The notion of value interface represents economic reciprocity, meaning that *all* value ports transfer objects of value, or *none at all.* For example, when provider A obtains interconnection from provider B, provider A will pay, as described by the contract, in the contract period. The same holds the other way around: If provider B is paid, provider B provides the interconnection service as described by the contract.

Finally, the *e*^{3}*value* contains the notion of *dependency paths.* Such a path consists of *consumer needs*, value interfaces, value transfers *connection elements* (visualized as straight lines in the *interior* of an actor), and *boundary elements*[2]. A dependency path shows which transfers must happen, as a result of a consumer need. It does not show *when* they will happen, only *that* they will happen in the contract period described by the model. This is sufficient to estimate economic profitability in the contract period.

The technical and business processes by which these transactions are implemented contain a lot more detail and are not shown [4]. It is even possible that the coordination processes that implement the commercial transactions implement a value transfer between actors A and B by means of a coordination process involving actors A, B and C. An *e*^{3}*value* model abstracts from these operational details and shows commercial transactions only.

In Figure 1, user A needs to make a call to User B. In exchange for the call, User A pays a sum of money. By following the dependency path, we can see that provider A should obtain interconnection to provide the telephone call, and should pay for this interconnection. Finally, provider B delivers a telephone call service to user B.

For now, it is important to understand that in this *e*^{3}*value* model *all* transfers on a dependency path are assumed to occur. In other words, the model shows what happens in reality, only all actors behave as agreed and expected. So, actors are always paying, and services are always provisioned. That is why we call such a model an *ideal* model; all actors operate honestly.

3.3 Construction of Sub-Ideal Business Value Models

In real-life, actors do not always behave as agreed and expected. They can perform intentionally or unintentionally in a different way. For example, an actor

[2] A dependency path also may contain *AND*, *OR*, and *explosion/implosion* elements to represent dependency splits and joins, but for explanatory purposes, these are not used in Figure 1.

may not pay, or pay a wrong amount of money. Currently, in e^3fraud, we consider two types of *intended* misbehaviours:

1. Transfers which should happen in the ideal model, do not happen at all in reality;
2. Transfers that happen in reality are not supposed to happen in the ideal model;

Furthermore, actors assumed to be independent in the ideal model may collude.

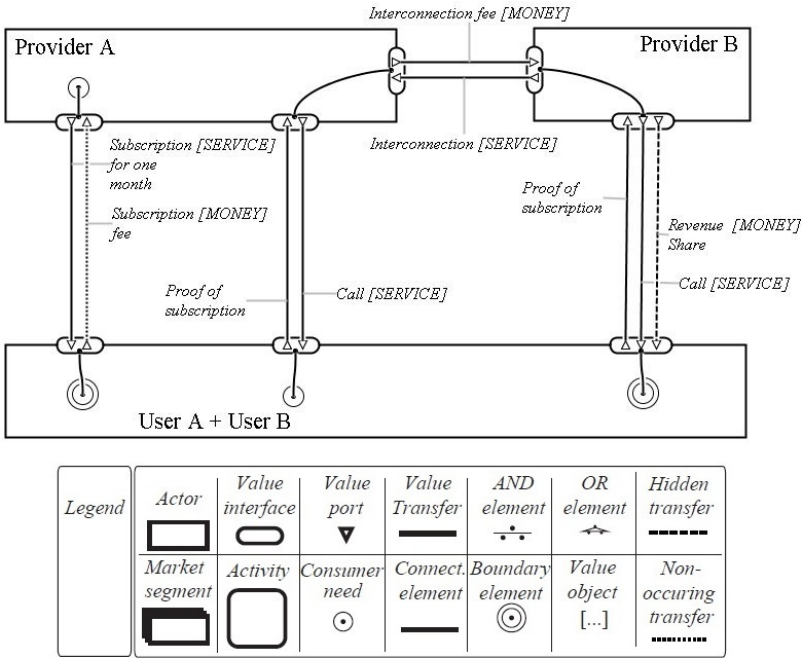


Fig. 2. Sub-ideal model: User A calls himself and earns money

We construct sub-ideal value models from the point of view of the same actor, in this example provider A, who is the ToA. A sub-ideal model represents the business value model as seen by the attacker and is created by changing the ideal model to represent misbehaviour.

Figure 2 shows an example of revenue sharing fraud, exhibiting both types of misbehaviours described above, as well as collusion. Rather than two end-users, as shown in Figure 1, we have now a single end-user A, who is exhibiting unwanted behaviour. This end-user has the same monthly subscription with Provider A as outlined in Figure 1. It is important to understand that this monthly subscription is based on a flat-fee tariff, which allows the user a to place a unlimited number of calls for free.

However, user A *also* has also access to a telephone hosted by provider B. The contract between user A and provider B states that for *received* call, user B gets

part of the interconnection fee obtained by provider B (*Revenue Share)*. This is a common arrangement for 0900 numbers. Again, since we take the point of view of Provider A, we have no information on how User A obtained a contract with provider B or what the structure of their agreement is. For the fraud analysis, it is sufficient to assume such a bonus is being paid. Furthermore, since the bonus pay-out is hidden to Provider A (the ToA), it is represented using a *dashed* line. Note that user A only uses provider B to *receive* calls.

To make matters worse, in this sub-ideal scenario we assume User A does not intend to pay his monthly fee to Provider A. As it is a non-occurring transfer with respect to the ideal model of the ToA, the *Subscription Fee* value transfer is represented using a *dotted* line.

User A will now place as many calls as possible per month with provider B. As can be seen by following the dependency path, the *same* user A also terminates the call, but with his phone hosted by provider B. For each terminated call, user A receives a bonus. Considering that, in addition, he also intends to default on his payment of the Subscription fee, he is the position to make a a generous profit.

3.4 Financial Analysis of the Attack

The most important financial factors of Telecom fraud, with regard to Risk Assessment are: (1) losses incurred by the provider and (2) motivation (in terms of potential gain) of the attacker. The former allows for estimating the impact of each type of fraud, while the latter is a critical part in estimating the likelihood of such a scenario taking place. The likelihood and impact of a fraud scenario can be used to compute the overall Risk associated with each particular scenario.

To estimate these factors, we need to analyse a pair of models: an ideal model showing the e^3value model of normal usage and a sub-ideal one showing the e^3fraud model of fraudulent usage. Furthermore, in pay-per-usage environments, such as telecom, the magnitude of the risk is dependent on the scale of usage (e.g. minutes called).

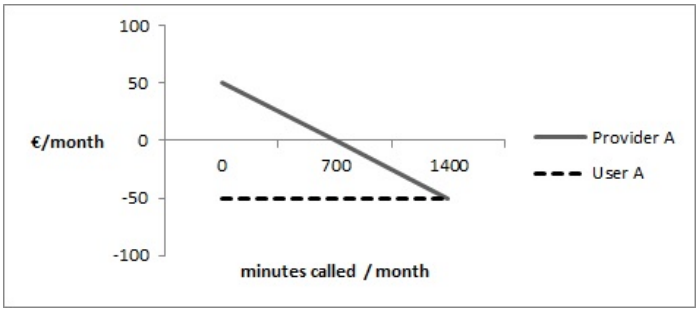
A custom software tool was developed that takes as input two models and generates profitability graphs for both the ideal and sub-ideal case(s) showing the dependency of the profitability with regard to usage. This allows for a visual comparison of ideal vs. non-ideal business cases of the provider as well as regular vs. fraudulent business case for the customers (and potential fraudsters) across a given range of occurrence rates.

The two graphs in Figure 3 are generated by this tool from the models shown in Figures 1 and 2. Realistic and, where available, real, values were used to instantiate the models. The chosen values are based on tariffs charge by Dutch Telecom providers in 2014. For simplicity, we only show the financial result of user A and Provider A (vertical axes), relative to the number of calls made (horizontal axis).

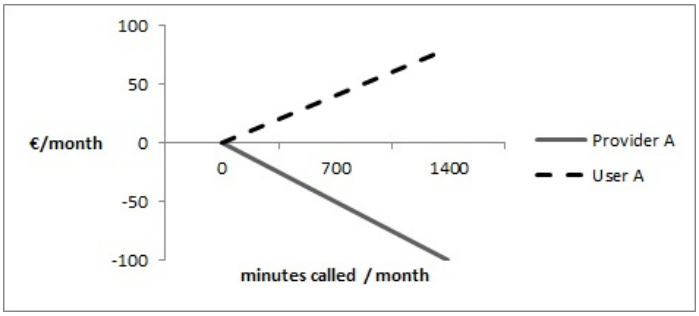
The financial outcome expected by the Telecom provider, in normal usage conditions, is visible in Figure 3a. Here, the user has a fixed cost, the monthly cost of the subscription. The costs of Provider A increase with each call, due

to the termination bonus paid to Provider B for the interconnection. Operating costs are not represented here as they are unknown and assumed to be negligible for an individual user, but could be easily included in the model. The sub-ideal case (Figure 3b) is significantly different. Besides the clear loss for the provider, the fraudster's financial motivation is now clearly visible.

While the value model(s) alone do not contain sufficient information to reliably elicit procedural or technical countermeasures on it's own, these financial results can be used to discuss checks on the non-occurring transactions or infer thresholds based on break-even points so as to mitigate the Risks.



(a) Ideal case



(b) Sub-ideal case

Fig. 3. Profitability graphs of the RSF scenario

4 Using the *e*^{3}*fraud* Approach to Analyse Technical Risks

Real-world security risk assessments typically result in the identification of a list of risks that is too long to be mitigated completely. The assessors must therefore prioritize the risks and mitigate only the most "important" ones. Importance is usually estimated by factoring in attractiveness of a potential attack to the attacker with the amount of loss caused by the attack. In this section, we demonstrate how the *e*^{3}*fraud* approach could be used to complement a Risk Assessment

of the infrastructure by facilitating impact as well as the gain estimation of individual risks, based on ranges of variables.

The alternative approach described in this Section takes as input a technical risk described in terms of an ideal model (before the attack) and a sub-ideal model (after the attack) and produces graphs showing the financial loss/gain related to the Risk.

4.1 Scenario Description

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 [20]. By exploiting vulnerabilities in a company's PBX, fraudsters may obtain access to one or more of an organization's phone numbers, which they can then use for personal, often fraudulent, purposes. Although attacks on the phone infrastructure are not as notorious as the revenue share fraud analysed above, reports show they are as likely to occur as an attack on the data network [17].

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, a fraudster can create a special mailbox which redirects him to a phone number of his choice. This number could be either a premium-rate (0900) number owned by a criminal organisation the fraudster is part of or a number that provides the callee with a revenue share for every received call.

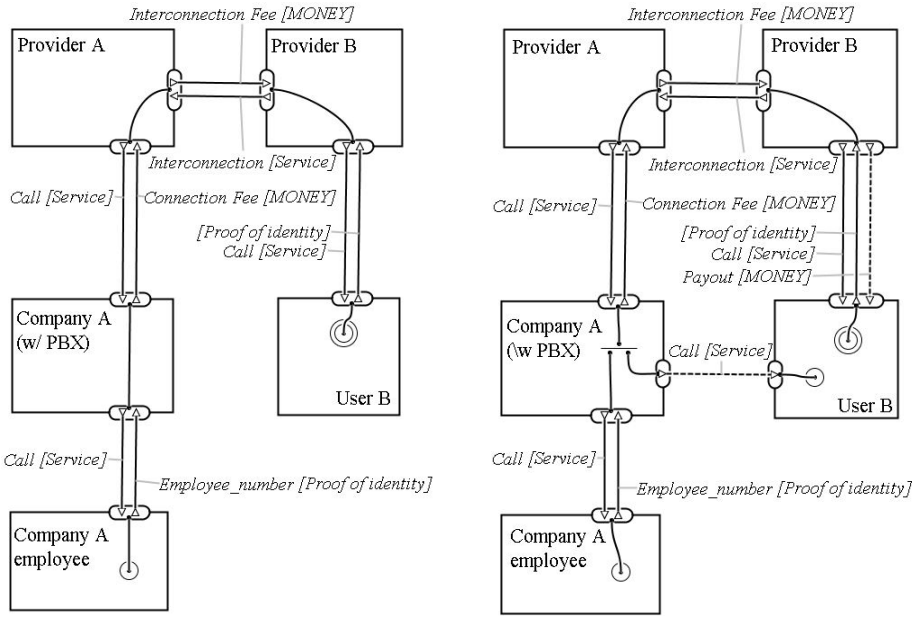
Another option would of course be to obtain possession of a telephone within the company and start calling his number from there [15]. One way to do this is to blackmail or bribe a company employee. In e^3fraud, we abstract from the technical or social means to access a company's phone number, and concentrate on the business model for the attacker.

4.2 Construction of Ideal and Sub-ideal Business Value Models

We want to estimate the potential loss the company would face in case of unauthorized access to it's PBX, as well as the potential gain a malicious actor with such access could obtain.

To start, we create an ideal model of the value exchanges as perceived and expected by the Target of Assessment, whose perspective we take. In this case, we take the perspective of the Company who owns the PBX. We want to estimate the potential loss the company would face in case of unauthorized access to it's PBX, as well as the potential gain a malicious actor with such access could obtain. Figure 4a shows the ideal model: Employees (Company A employee) may call through the company PBX to external Users (User B). This is the normal usage the company expects, given honest actors.

Next, we tweak the model to show the commercial traces of the risk we want to analyse. For example, Figure 4b shows a sub-ideal model where User B is an



(a) Ideal model: Employee calls User B

(b) Sub-Ideal model: User B uses illicit access to PBX to call himself

Fig. 4. Models used to analyse the Risk of PBX hacking

attacker. He obtains access to the PBX (dashed line) and exploits this (illicit) access order to make calls to through a provider that pays out a reward for every call received.

It is interesting to note that the value model abstracts away from the actual vulnerability being exploited and the process by which access is gained. In order to fully describe the attack, a coordination model such as an attack tree is needed.

To do a financial analysis of the risk, we instantiate both models with known or realistic values and use the e^3fraud computation engine to generate profitability graphs showing the financial result of all actors involved for both the ideal and sub-ideal case, similar to the ones shown in Figure 3.

By contrasting the financial result of *Company A* in the ideal model with its financial results in the sub-ideal model, we can quantitatively estimate the *impact* associated with a technical risk. Furthermore, by computing the financial result of the attacker in each sub-ideal case, we can estimate the expected *gain* of each attack. It is worth noting that the costs of setting up the attack are not taken into account and thus we cannot claim to estimate the attack's *profitability* (as *costs-gain*).

Using the software tool described in Section 3.4, we can generate a multitude graphs, for various ranges of malicious calls.

Tweaking model parameters and re-running the tool also provides an efficient way of conducting sensitivity analyses.

Because e^3fraud models abstract away from the technical means of conducting an attack, there is reason to believe e^3fraud models might be re-usable, meaning the overhead of creating such a model for each Risk would not be significant.

5 Discussion and Conclusions

We have shown how business value models can be used to identify and quantify risks of fraud in e-service networks, where information about the technical infrastructure of the partners in the network is incomplete or even absent.

In particular, e^3fraud, a proof-of-concept extension of e^3value, is able to identify, model and analyse business risks, as well as quantify the business impact of technical or procedural risks.

5.1 Validity

The approach presented in this paper has been successfully applied to four Telecom fraud scenarios, containing a variety of business as well as technical risks. The models were validated with the help of the scenario owners. Results matched existing estimations and by using real values we were able to show that at least one instance Revenue Sharing Fraud is still possible today.

The approach was also demonstrated to domain experts working for the fraud department of a leading Telecom provider and received positive feedback. The method was generally perceived as useful, especially for quickly assessing the financial fitness of new plans before they are launched and estimating the impact of new types of fraud on existing plans. Furthermore, the experts saw the profitability graphs as an expressive means of communicating risks to product managers.

However, experts envisage several functional improvements before the e^3fraud method and toolkit would be usable in practice: the ability to model a larger variety of sub-ideal models (such as ones containing hidden actors) and the possibility of automatically generating and ranking sub-ideal models based on a given ideal model. Finally, a library of model patterns was mentioned as a way to promote (re)usage.

5.2 Limitations

While e^3fraud can be used to help reduce possibilities of fraud on the service level, as well as to quantify some known infrastructure risks, it does not necessarily help to identify attack on the technical infrastructure, such as a DDOS attack. e^3fraud is especially applicable in cases where the economics of risk are of particular importance, such as for analysing fraud that takes place on the service level rather than the technology level.

The biggest strength of e^3*fraud* models - similar to the e^3*value* models they build upon - is also their biggest weakness: they abstract away from any and all procedural and architectural information. 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.

Even though the order of execution is not important for the business model, to discuss countermeasures, we need to be able to reason about the coordination processes and IT architectures that can mitigate risks. In general, transformation to or generation of any sort of architecture or coordination model from an e^3*value* model is not feasible [4]. There exists previous work discussing these relationships for [16, 8, 5, 19, 14, 6]. However, none of these papers are about (in-)security or fraud and mostly assume ideal business environments. This motivates a closer study of the relation between e^3*fraud* models, coordination models, and enterprise architecture which are relevant or useful in the context of Risk Assessment.

Finally, this work is still in its initial stages. As the methodology and tool have been developed and tested on a limited number of telecom fraud scenarios, the approach is somewhat example-driven. Thus, an obvious next step is to model and analyse a larger variety of scenarios so as to further develop and validate the idea.

5.3 Generalisability

We have developed and illustrated the e^3*fraud* approach on a number of cases from telecom service provision. To which extent is this generalizable to other kinds of e-service provision? At the moment we can only speculate about this, but the true test of generalizability is the application of e^3*fraud* to other kinds of e-service provision networks. We plan to do this in future work. In the absence of any such empirical evidence, we analyse the features of the studied telecom service networks that make e^3*value* and e^3*fraud* suitable to identify and analyse business risks.

In the telecommunications sector, information on the technical infrastructure of competitors is unobtainable, which makes e^3*value* and e^3*fraud* well-suited to model business risks. Describing the money flows and their triggers is necessary and sufficient to understand such scenarios and not only derive estimates of both impact for the provider and gain for the fraudsters, but also identify countermeasures.

A second characteristic of the telecom sector is the importance of a short time-to-market. The marketing department of a Telecom provider typically wants to launch new services 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. Our initial

evidence shows that e^3fraud offers the promise to offer efficient support in risk identification and mitigation. To further improve this efficiency, we are currently working on automatically generating and ranking the sub-ideal models.

Based on this brief analysis of the factors that contribute to the usability and usefulness of e^3fraud in the identification and analysis of risks of fraud in telecom service provision, we speculate that e^3fraud will be equally useful in other cases of e-service provision where information about the technical infrastructure of competitors is unobtainable, time-to-market of new services must be short, and losses created by instances of fraud must be kept within acceptable bounds. We plan to do case studies that provide evidence for this speculation in future research.

Acknowledgements

The ideas and models presented here were developed with the support of S. Koenen and Dr. M. Daneva of the University of Twente. This research has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TREs- PASS). This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.

References

1. D. Baker. International revenue share fraud: Are we winning the battle against telecom pirates? *Black Swan Telecom Journal*.
2. D. Freedman. The phone hacking scandal: Implications for regulation. *Television & New Media*, 13(1):17–20, 2012.
3. J. Gordijn and H. Akkermans. Value based requirements engineering: Exploring innovative e-commerce idea. *Requirements Engineering Journal*, 8(2):114–134, 2003.
4. J. Gordijn, H. Akkermans, and H. Van Vliet. Business modelling is not process modelling. In *Conceptual Modeling for E-Business and the Web, ECOMO 2000*, volume 1921 of *LNCS*. Springer, 2000.
5. J. Gordijn and H. Van Vliet. 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*, 1999.
6. J. Gordijn and R. Wieringa. A value-oriented approach to e-business process design. In *Proceedings of the 15th International Conference, CAiSE 2003*, volume 2681 of *LNCS*, pages 390–403. Springer Verlag, 2003.
7. D. Ionita, P. Hartel, W. Pieters, and R. Wieringa. Current established risk assessment methodologies and tools, September 2013.
8. W. Janssen, R. van Buuren, and J. Gordijn. Business case modelling for e-services. In D. R. Vogel, P. Walden, J. Gricar, and G. Lenart, editors, *Proceedings of the 18th BLED conference (e-Integration in Action)*, pages cdrom,, Maribor, SL, 2005. University of Maribor.

9. V. Kartseva. *Designing Controls for Network Organization: A Value-Based Approach*. PhD thesis, Vrije Universiteit Amsterdam, 2008.
10. V. Kartseva, J. Gordijn, and Y.-H. Tan. *Designing Value-based Inter-organizational Controls Using Patterns*, volume 14 of *LNBIP*. Springer Verlag, 2009.
11. D. R. Kuhn, N. I. of Standards, and T. (U.S.). *PBX vulnerability analysis [microform] : finding holes in your PBX before someone else does / D. Richard Kuhn*. U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology ; For sale by the Supt. of Docs., U.S. G.P.O Gaithersburg, Md. : [Washington, D.C, 2001.
12. K. Mohan and B. Ramesh. Ontology-based support for variability management in product and service families. 2003.
13. R. Normann and R. Ramírez. *Designing Interactive Strategy - From Value Chain to Value Constellation*. John Wiley & Sons Inc., Chichester, UK, 1994.
14. V. Pijpers and J. Gordijn. 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*, page cdrom. Computer Society Press, 2007.
15. T. Regan. Pbx security in the voip environment. `http://www.spitfire.co.uk/pdf/05_PBX_Security_in_the_VoIP_environment-white_paper_140313_2.pdf` accessed Nov 2014, March 2013.
16. P. M. Singh. Integrating business value in enterprise architecture modeling and analysis, August 2013.
17. SMARTVOX. How secure is your asterisk pbx? `http://kb.smartvox.co.uk/asterisk/secure-asterisk-pbx-part-1/` accessed Nov 2014, 2014.
18. R. Wieringa. *Design Science Methodology for Information Systems and Software Engineering*. Springer, 2014.
19. R. Wieringa and J. Gordijn. Value-oriented design of correct service coordination protocols. In *Proceedings of the 20th ACM Symposium on Applied Computing*, pages 1320–1327. ACM Press, 2005.
20. Wikipedia. Business telephone system — Wikipedia, the free encyclopedia, 2014.