Fraud Risk Modelling: Requirements Elicitation in the Case of Telecom Services

Yesuf, Ahmed; Wolos, Lars Peter; Rannenberg, Kai

Published in:
Exploring Services Science

Link to article, DOI:
10.1007/978-3-319-56925-3_26

Publication date:
2017

Document Version
Peer reviewed version

Link back to DTU Orbit

Citation (APA):
Yesuf, A., Wolos, L. P., & Rannenberg, K. (2017). Fraud Risk Modelling: Requirements Elicitation in the Case of Telecom Services. In *Exploring Services Science* (Vol. 279, pp. 323-336). Springer. https://doi.org/10.1007/978-3-319-56925-3_26

Fraud Risk Modelling: Requirements Elicitation in the Case of Telecom Services

Conference Paper *in* Lecture Notes in Business Information Processing · April 2017

DOI: 10.1007/978-3-319-56925-3_26

Ahmed Seid Yesuf
Goethe-Universität Frankfurt am Main

Lars Wolos
Goethe-Universität Frankfurt am Main

Fraud Risk Modelling: Requirements Elicitation in the Case of Telecom Services

Ahmed Seid Yesuf[1], Lars Wolos[2], and Kai Rannenberg[1]

[1] Deutsche Telekom Chair of Mobile Business and Multilateral Security,
Goethe University Frankfurt, Frankfurt am Main, Germany
{ahmed.yesuf,kai.rannenberg}@m-chair.de,
[2] Department of Applied Mathematics and Computer Science,
Technical University of Denmark
lpwo@dtu.dk

Abstract. Telecom providers are losing tremendous amounts of money due to fraud risks posed to Telecom services and products. Currently, they are mainly focusing on fraud *detection* approaches to reduce the impact of fraud risks against their services. However, fraud *prevention* approaches should also be investigated in order to further reduce fraud risks and improve the revenue of Telecom providers. Fraud risk modelling is a fraud prevention approach aims at identifying the potential fraud risks, estimating the damage and setting up preventive mechanisms before the fraud risks lead to actual losses. In this paper, we highlight the important requirements for a usable and context-aware fraud risk modelling approach for Telecom services. To do so, we have conducted two workshops with experts from a Telecom provider and experts from multidisciplinary areas. In order to show and document the requirements, we present two exemplary Telecom fraud scenarios, analyse and estimate the impacts of fraud risks qualitatively.

Key words: fraud risk, requirement elicitation, fraud modelling, service security, telecommunication, risk assessment

1 Introduction

Telecom providers are losing billions of dollars every year due to frauds. According to the Communications Fraud Control Association (CFCA), the global revenue of Telecom providers was affected by almost $38.1 billion (USD) in the year 2015 [1] due to frauds. Fraud is the use of a Telecom service to gain money or with no intention to pay. There are many types of Telecom frauds. The top five types mentioned in the 2015 CFCA report are International Revenue Share Fraud (IRSF), interconnect bypass, premium rate services, arbitrage and theft/stolen goods. IRSF costed the Telecom providers almost $10.76 billion (USD) globally in the year 2015 [1], which is almost threefold from the year 2011.

Telecom providers store subscribers usage behaviour - known as call data records (CDR) - in a database. Telecom fraud detection systems (FDSs) usually use anomaly-based fraud detection relying on identifying anomalies through comparing the past and current or recent behaviour of subscribers [2, 3, 4]. Although a FDS has advantages, it has also a problem of detecting frauds only once a fraudster follows a predefined and/or behaviour-based pattern stored in the detection system – which increases the reaction time if it happens in a larger scale. Given these and the (revenue-loss) figures above, it is not surprising that Telecom providers aim to reduce the damage. Thus, in order to predict fraud risks beforehand and take preventive measures, a fraud risk assessment approach is required as part of Telecom service security.

According to ISO/IEC 27005 [5] a risk assessment process starts from understanding the context and performing risk analysis. In terms of the Telecom domain, the risk assessment process begins by understanding the Telecom service under assessment, identifying the potential risks and estimating the consequences of those risks. We believe this process substantially helps to reduce the level of fraud risks before a given Telecom service is under attack. Basing on the general risk assessment process, the first step for a usable and context-aware fraud risk modelling approach is to elicit requirements necessary to develop the intended approach. The main contribution of this paper is, therefore, eliciting the important *requirements* for a context-aware and model-based fraud risk modelling at different stages of the assessment.

The rest of the paper is organised as follows. Section 2 provides background on the context of Telecom services and fraud risks. Section 4 describes the methodologies used in order to elicit the requirements of fraud risk modelling. Section 3 discusses the related work on security requirements in the Telecom domain. In Section 5, two exemplary fraud scenarios are described. We also performed a risk analysis on each scenario to show fraud enablers and document the initial requirements on fraud risk modelling. These requirements at different stages of fraud risk modelling are discussed in Section 6. At last, Section 7 summarises and concludes the important points in the paper and provides insights for future work on fraud risk modelling approaches.

2 Background: Telecom Services and Types of Fraud

The core elements of Business Process Management (BPM) in a Telecom provider involve “products” (actually services) and the infrastructures to “produce” them [6]. The other elements of the BPM are based on these core elements - the operations, marketing and service delivery management [6]. Telecom services include call services (mobile and fixed-line), roaming services [7], data services, Internet services (e.g. VoIP service) and messaging services.

When taking a closer look, most Telecom services require a complex technical network architecture. This is due to a multitude of different interconnected networks, network operators and service providers. At the same time, in most cases, the underlying business models are tailored to compete in highly competitive markets. This entails opposed financial interests of the participants and very often even more complex services. Furthermore, this proves fertile ground for fraud or misuse.

Telecom frauds affect both fixed line and mobile services which could be provided through either prepaid or post-paid contracts [8][9][4][10]. There exist several categories of fraud in the literature, e.g. [11], [12], [13] and [14]. Some of the known methods that fraudsters use to commit fraud include:

PBX hacking: A Private Branch Exchange (PBX) is a telephone network used within a company to switch calls coming from outside the company rather than installing individual telephone lines to each user in a company - which is very expensive. Fraudsters identify the potential weaknesses of PBXs to forward calls from the outside network, as PBXs provide the capability to remotely connect to a central portal (voicemail) [15][16]. According to CFCA [1], the damage of PBX hacking in the year 2015 is estimated to $3.93 billion (USD).

Subscription fraud: This is another typical method of committing fraud [3][4]. It happens through using users' information illegally either through scamming or other forms of social engineering attacks. According to CFCA [1], the damage of subscription fraud in the year 2015 is estimated around $3.53 billion (USD).

Wangiri fraud: Wangiri fraud, originated in Japan, is also known as "one ring and cut" fraud which makes everybody a target by making calls and waiting for a reply [17]. When victims call back, they would listen to advertisements from a premium internet service or calls. This will cause expensive bills to the users who call back to the missed-call.

In the paper, we focus on business-related fraud risks and used the following definitions.

– Telecommunications Service Provider (TSP): A TSP covers the different types of providers of Telecom services, regardless of whether they operate a network by themselves or just (re)sell services.
– Call termination: Call termination is a service of a TSP to route phone calls from another TSP to customers of the first TSP. Call termination could happen for national and international calls.

3 Related Work

Ensuring the security of a system is a fuzzy challenge but through procedural techniques, the level of system or service security can be improved. One way is through "implementing" security requirements using security engineering methods. Unfortunately, traditional risk analysis and security engineering methods have several limitations when applied to Telecom cases [18]. Zuccato et al. [18] proposed a security requirement engineering method - SKYDD - including infrastructure, business and information requirements based on checklists, guidelines and expert knowledge. In continuation to this work, Zuccato et al. [19] proposed an approach which is a step by step process to use service security requirement profiles. They outlined four basic requirements for the approach: economic feasibility, agility, multi-disciplinity and help without the need for security experts.

The approach is, therefore, intended to span all kinds of security issues (mostly related to business related risks).

Tian et al. [20] presented a requirement model not for the security domain but for a solution domain in the Telecom field such as an SDP (Service Delivery Platform). This domain requirement model allows producing a model that can be easily navigated through its hierarchical structure to incorporate featured and detailed requirements for stakeholders and developers respectively. In relation to the usage of Telecom services, Krogstie [21] highlighted the areas to focus in order to cope with the technology shifts of mobile information systems. He described the advantage of involving the concept of mobility and people's involvement (the context) in mobile information systems using requirement engineering mechanisms.

In general, even though there is a limited amount of literature in the area of Telecom service security, some of the papers above have some relation with security and requirements engineering. Still, none of the papers focuses on preventive risk modelling requirements to deal with fraud risks. Recently, we showed a risk analysis using a value-based approach [22]. As a continuation to cover identification, analysis and estimation of fraud risks, this paper highlights requirements on fraud risk modelling for the case of Telecom services.

4 Methodology

To elicit the requirements on fraud risk modelling, we have conducted two workshops. In total, eleven experts have attended the workshops. Four of them are experts from a TSP who have experience of Telecom fraud and seven of them are security researchers from inter-disciplinary fields (information security, computer science and mathematics). On first sight the number of involved experts may look small. However due to the high secrecy requirements of anti-fraud measures it is actually quite difficult to conduct workshops like these, where several experts in front of researchers discuss issues and even contribute different opinions in a single session. Therefore, the workshop lead to results, that are novel, even though the quantitative base is not the largest.

The first workshop was conducted with the experts from the TSP (seven participants including the authors for three hours). The workshop was conducted with a moderated discussion where the people from the TSP presented different types of Telecom fraud (revenue-share fraud, roaming fraud, call selling fraud and PBX fraud). In the discussion session, they also discussed the effects of those frauds to the TSP. Through questioning and answering, they discussed their expectations of fraud prevention approaches to reduce the effects of fraud to the TSP. In this paper, we present two of the fraud scenarios to show how we elicited the requirements on fraud risk modelling.

Taking their expectations, in the second workshop – where only security researchers met with eight participants for three hours – we formulated problems of those example fraud scenarios, identified the potential fraud enablers, estimated qualitatively the impacts of the fraud scenarios on the Telecom. The main outcome of this workshop was a list of initial requirements for a risk modelling approach. A risk modelling approach consists of three main components: conceptual model, analysis and estimation. The requirements are covering all of the three components.

5 Analysis of Exemplary Fraud Scenarios and Expectations of TSP

In this section, two exemplary revenue-share fraud scenarios are presented and analysed to show how we have elicited the requirements on a risk modelling approach for Telecom services. We also discussed the expectations of the TSP expressed in the first workshop. We chose the two exemplary fraud scenarios because they show very well: 1) the involvement of several actors and entities to commit a fraud; 2) chain(s) of fraudulent activities in a simplified way; 3) money flows (fraud risks) of fraudulent actors; and 4) the contribution of technological weaknesses to fraud risks. Some other fraud scenarios can be found in (e.g. [22]).

5.1 Exemplary Fraud Scenarios

Customers of TSPs in possession of insider knowledge could identify possible arbitrage scenarios by combining TSP services and products (often involving multiple TSPs). One prominent example is the use of flat-rate tariffs for call termination. Another example is the involvement of weak identity checks for new connections to enable a portfolio of usage scenarios that violate at least the terms and conditions of the TSPs involved, which results in a profit for the fraudster. We are using these two example scenarios to show how we documented the requirements on the risk modelling. For both scenarios, even though the net loss of a TSP resulting from a single customer's usage pattern is not a problem per se for the respective TSP, a large-scale systematic exploitation of such a scenario however will add up to a critical level.

Fraud scenario 1 - Tariff misuse for call termination

Mr. Clever, a fraudster, has (multiple) fixed, mobile or virtual IP connection points with TSP A. These are billed either as flat-rate or in tariff schemes which include capacious minute budgets. Also, Mr. Clever has (multiple) fixed, mobile or virtual IP connection points with TSP B. Call termination fees are paid on a per minute basis by TSP A when calls are delivered from TSP A to TSP B. TSP B passes a part of the received call termination fees to Mr. Clever, thereby providing a payout per minute for incoming calls as incentive to generate as much incoming traffic as possible to the network of TSP B. This process is mostly done by an intermediary company, whose main activity is bridging between the fraudster and fraudulent TSPs. Mr. Clever makes calls from TSP A to TSP B in order to maximise his profit from these payouts. The money flow is shown in Fig. 1. The source of Mr. Clever's profit is the *call termination fee* paid by TSP A to TSP B, which is then partly paid out to Mr. Clever by TSP B (Mr. Clever's costs at TSP A are fixed due to the chosen tariff).

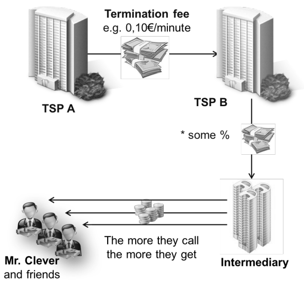

Fig. 1. Money flow for scenario 1

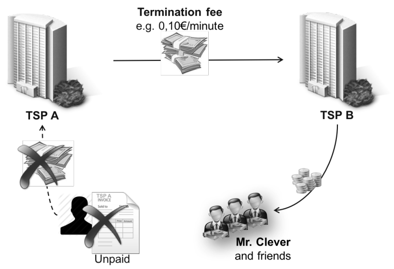

Fig. 2. Money flow for scenario 2

Fraud scenario 2 - fraud involving the false pretence of being willing and able to pay

This scenario can be described in five sequential steps.

1. Mr. Clever obtains a high number of prepaid (pay as you go) SIM cards. These SIM cards are either not (yet) registered or registered using fake or stolen IDs. Furthermore, these SIM cards are billed either as flat-rate, have a very low price per minute, or have free minutes (upon activation). In addition to these prepaid SIM cards, Mr. Clever manages to establish one post-paid mobile contract with TSP A using a fake ID or forged identity and bank card credentials. Thus, with respect to the post-paid mobile contract, this scenario is a matter of fraud involving the false pretence of being willing and able to pay.
2. Mr. Clever activates call forwarding on the post-paid mobile connection point to a (foreign) external TSP B. He then makes the highest number of possible parallel calls to that post-paid mobile connection point using the above prepaid SIM cards. All calls will be diverted to TSP B. Call termination fees are paid on a per minute basis by TSP A when calls are delivered from TSP A to TSP B.
3. The fraud detection system (FDS) of TSP A may detect the violation of limits on the post-paid mobile connection contract and disconnect it within the response time.
4. Mr. Clever does not pay the post-paid bill.
5. TSP B passes a part of the received call termination fees on to Mr. Clever, thereby providing a payout per minute for incoming calls. The money flow is shown in Fig. 2.

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

5.2 Fraud Risks: Partial Risks from the Exemplary Scenarios

For the two scenarios presented in Section 5.1, we have discussed the (partial) risks identified in the workshop which allow a fraudster to perpetrate the fraud.

Risks are named *partial* as their discrete or isolated occurrence would not necessarily be relevant to the company while multiple risks constitute a (relevant) fraud scenario. We have then estimated qualitatively the partial risks based on their contribution to the occurrence of the fraud scenarios. For the sake of simplicity, we decided to use a risk estimation scale with three values: *High, Medium* and *Low*. A *High* rating has a significant contribution to the occurrence of a fraud and has impact at least on one of the dimensions (e.g. reputation, money, etc.). *Medium* and *Low* means less contribution and impact. The identified partial risks are described below.

R.1 Weak identity checks enable a fraudster to acquire a high number of prepaid (pay-as-you-go) SIM cards using fake IDs: Sound identity and credit checks are costly. Due to high pricing pressure in the Telecom market, the economically reasonable level of effort is limited. This holds true especially for prepaid (pay-as-you-go) SIM cards, leading to a higher risk of identity fraud.

- Impact: *High*
- Initial requirement: the risk modelling approach should model the processes of acquiring different types of Telecom connections and identify fraud risks due to weak identity checks.

R.2 A fraudster manages to mask fraudulent calls to simulate legitimate traffic: Fraud detection systems (FDSs) are operated by TSPs to detect excessive usage of their network resources. In a case of misuse, the FDS should detect the violation of limits, e.g. multiple long-lasting connections of similar length or to the same destination number. Distributing calls using multiple destination numbers and a random duration would mask the fraudulent activity making it much harder to detect.

- Impact: *High*
- Initial requirement: the risk modelling approach should model the possible actions in the existing fraud detection mechanisms, identify the potential risks against such mechanisms and analyse their impact.

R.3 A fraudster acquires a post-paid contract using fake IDs: Stolen identity documents and bank account information enable fraudsters to sign up for a post-paid contract. Factors which facilitate this are: Contract concluded online, sloppy work of retail personnel, acceptance of copied identity documents.

- Impact: *Medium*
- Initial requirement: the risk modelling approach should model the processes how customers or fraudsters acquire different types of connections (including post-paid) and identify weak points that create fraud risks.

R.4 A fraudster manages to find a TSP B which provides payout: There are different TSPs in the market offering payments and incentives to their customers for incoming calls. These incentives need to be usable in a profitable scenario with the products of a TSP A in order for the fraudster to make a profit.

- Impact: *High*
- Initial requirement: the fraud risk modelling approach should incorporate the influences of external services. In reality, this might be difficult to achieve, but

with existing data about the external services, it is possible to estimate the damage of the external influence.

R.5 High response time of TSP A's implemented fraud detection system (FDS): Depending on the implementation of the FDS, response times may vary between 15 and approximately 60 minutes.
- Impact: *Low*
- Initial requirement: besides modelling the possible actions, the fraud risk modelling approach should model the response time of fraud detection mechanisms in order to analyse and estimate the impacts of a fraud.

R.6 A new product thwarts the business model of existing products: A TSP launches a product without properly considering its side-effects and interdependencies with existing products and the resulting user behaviour.
- Impact: *Low*
- Initial requirement: the fraud risk modelling approach should incorporate impact analysis of new products to the existing models.

5.3 Expectations of TSP Experts

New Telecom services usually have to be launched under significant time pressure, e.g. to minimize the time-to-market or to react swiftly to a move of a competitor. This leaves little time and space to account for potential misuse. As discussed in Section 5.2, misuses could happen due to sloppy (service) design, underestimation, or misjudgement of the extent of possible exploitation by fraudsters and their motivation to find combinations of different services often involving multiple providers. Based on the discussion in the workshop with the TSP experts, they expect that a preventive approach to:

- identify as many misuse scenarios as possible to find out whether a service is reasonably profitable;
- minimise potential risks associated with the service (and, as a result, potential losses);
- work as a preventive solution or technique for dealing with potential fraud related to Telecom services before it is exploited (in a large scale).

6 Requirements on Fraud Risk Modelling

Based on the outcomes of initial requirements and the expectations of the TSP, we propose a fraud risk modelling approach (cf. Fig. 3). This fraud risk modelling approach involves representation of service, identification and analysis of potential fraud risks and estimation of their impacts. The fraud risk assessment starts with modelling the context of the TSP service under assessment in a *conceptual model* – a model which represents the context of the target of assessment to the intended level of abstraction. Through this conceptual model, a fraud analyst is able to communicate, identify fraud risks and estimate potential damages. Taking this into consideration, the first three subsections in the following describe

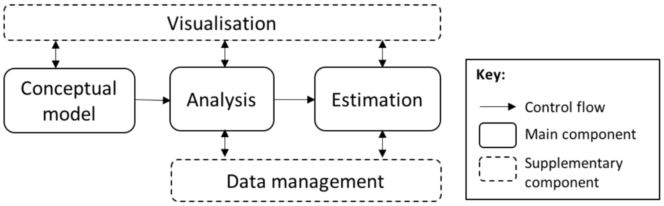

Fig. 3. Components in the fraud risk modelling approach

the requirements of each component in the fraud risk modelling approach (conceptual modelling, fraud analysis and estimation) followed by supplementary requirements (data management and visualisation).

The requirements at each component should generally be evaluated based on the following criteria:

- *context-awareness* – the ability to include internal and external factors in the analysis of a Telecom service;
- *representativeness* – the capability of representing essential elements of the target of assessment;
- *scalability* – the ability to handle complex Telecom cases with a reasonable performance;
- *usability* – the ability to support users efficiently and effectively. This includes the ability to generate the potential fraud risk scenarios and prioritise them. It also includes the capability of using different data formats in the assessment process.

6.1 Requirements on the Conceptual Model

As shown in the example scenarios above, the context of a TSP service includes several independent stakeholders, contract agreements between them, anti-fraud agents, Telecom employees, hardware and software, virtual communications, and network infrastructures.

The model needs to be able to represent a list of relevant properties of the entities (products and services) involved, including ownership of entities and a financial budget of the entities. The TSP service includes at least two parties (from now on we call them actors): subscribers and one or more service providers (TSPs). Subscribers receive a service with a short term or long term agreement provided by a TSP. The model, therefore, should represent contractual agreements and jurisdictional requirements.

For a roaming service, for instance, an additional external TSP is involved to fulfil the goals of the home TSP. Both the subscribers and the home TSP pay service fees. From the home TSP's perspective, a subscriber pays money for the service in different forms: prepaid, post-paid, or with some contractual agreement. The home TSP pays for the service given to its subscribers while roaming. These transactions between several independent actors create chances for fraudsters to perpetrate frauds or misuse the service. Therefore, the model should represent relations between different entities, as interrelations between different partial risks coincide and enable an attacker/fraudster to carry out an attack/fraud.

Depending on the type of a TSP service, the relevant entities should be identified and represented in the conceptual model, where the model serves as a medium of communication between, for example, the modeller and fraud analysts. Therefore, the model is expected to have formal or semi-formal semantics.

The *representativeness* of the model with respect to the service under assessment is in general the evaluation criterion to the requirements on the conceptual model. The following summarises the high-level requirements on the conceptual model. The conceptual model should represent:

- entities and their relevant properties, including ownership of entities and financial budget of the entities;
- the possible actions at each entity;
- relations between different entities, as interrelations between different partial risks may coincide and enable a fraudster to carry out a fraud;
- contractual agreements and jurisdictional requirements; the processes of acquiring different types of Telecom connections;
- the existing fraud detection mechanisms of the Telecom service in the model.

6.2 Requirements on the Analysis

Fraud analysis is the process of identifying the potential fraud scenarios and estimating the related potential economic damage to the TSP. Given the relevant entities in the contextual model of a TSP service, it should be possible to show or generate damaging incidents from the model. Damaging incidents have a damaging effect on the revenue of the TSP when implemented with a large enough level of scale. The analysis has to predict the possible fraud within a small amount of time before it amplifies the damage.

Depending on the type of a TSP service, the analysis process may leverage necessary data in relation to the contextual model - for instance, CDRs to analyse the fraud on fixed line call services. As the goal of the analysis is to predict potential fraud risks and propose preventive measures, it might leverage the usage-data in order to achieve this goal.

The analysis process should also incorporate the contractual and jurisdictional requirements on the TSP service under assessment. In the TSP service environments such as roaming, the jurisdictional requirements are crucial. In some countries, the delay in providing service usage files to the home TSP provides a chance for fraudsters to perform the fraud undetected for an extended time span. In some other countries, where Near-Real-Time Roaming Data Exchange is applied, the delay of the data exchange is limited to only four hours - if delayed the visited TSP is responsible for any kind of fraud detected after those four hours. Additionally, there are contract agreements in place between TSPs, covering subjects of interconnection fees and inter-operator charges. The fraud analysis, therefore, should consider both the contractual and jurisdictional requirements in order to predict the potential fraud risks in a TSP service.

Fraudsters use complex ways to perpetrate fraud in order to hide or legitimise their acts. Depending on the TSP service, the analysis approach should identify complex correlations of partial risks (cf. Section 5.2) to estimate the potential damage resulting from the fraud risks. The following summarises the high-level requirements on the analysis component. The analysis component should:

- identify fraud risks by identifying fraud factors from the conceptual model; different ways to identify fraud factors. To mention some: 1) by identifying the weaknesses of the components in the contextual model; 2) by using fraud patterns that fraudsters use as a guideline to identify fraud factors (e.g. due to weak identity checks). Evaluation criterion: *context-awareness* and *scalability*;
- consider contractual agreements and jurisdictional requirements in identifying the fraud risks. Evaluation criterion: *context-awareness*;
- handle complex correlations of partial risks. Evaluation criterion: *usability*;
- collect fraud scenarios identified due to fraud factors in a file format so that other fraud risk modelling components would use it (e.g. the risk estimation component to prioritise those fraud risks). Evaluation criterion: *usability.*

6.3 Requirements on the Risk Estimation

As explained in Section 5.3, new TSP products need to be launched under significant time pressure resulting from strong competition in a dynamic market, leaving little time and space to analyse and account for potential misuse of the product. At the same time, there is a (natural) conflict between on the one hand, the (marketing) department – responsible for product development and seeking business opportunities with a tendency to put a gloss on business case figures – and on the other hand, the misuse department – which has its focus on potential misuse and avoiding risks. In many organisations, these two departments act independently from one another and have different target functions.

Due to a persistent increase in product complexity, diversity on the feature side, and margin pressure on mass products, risks cannot be eliminated, but need to be assumed, estimated and accepted with some level of threshold, whilst minimising their possible impact. Hence, the focus of the risk estimation process should be on the question of calculability. The identified fraud scenarios should be estimated from different impact *dimensions*, mainly based on their economic impacts.

Basing on the types of the TSP services, the fraud risk modelling approach should have a framework for estimating fraud scenarios – either a qualitative or a quantitative estimation. TSP risks can qualitatively be represented in different levels of magnitudes. These magnitudes are interpreted based on the consequences of the fraud risk. As an example, High could be the loss beyond $10K, Medium between $10K and $4K, and Low below $4K. In the example scenarios (Section 5.2), we used three levels of qualitative measurement – High, Medium and Low to estimate the partial risks. Risk estimation using contextual models is usually qualitative but when it is supported by statistical and usage data, it could be expressed in terms of quantitative measurements. In general, a preventive fraud risk modelling approach should estimate those risks identified in the previous stage in either qualitative or qualitative measurements.

The following summarises the high-level requirements on the risk estimation. The risk estimation component should estimate:

- the impacts of the identified fraud risks based on different dimensions (e.g. its economic impact). Evaluation criterion: *usability*;
- the fraud risks in either qualitative or quantitative scale. Evaluation criterion: *usability*.

6.4 Requirements on Visualisation

In the course of fraud risk modelling, visualising inputs and outputs is necessary for a usable approach to facilitate decision making. Decision makers (commercial managers at the TSP) are interested in understanding the effect of fraud risks at a larger scale. To satisfy the goals of TSP stakeholders, visualisation requirements on fraud risk modelling are, therefore, important.

The approach should provide sufficient visualisation at different diverging aspects. A model should visually represent actors (economically or technically), assets, existing policies, the possible connections between actors, boundary restrictions and potential fraudulent actors. It should also depict, which part of the TSP service or product is vulnerable to a known type of fraud.

At the stage of fraud analysis, the approach should visually represent the costs of damage produced by the fraud on a given TSP service - for instance, in a graph where the likelihood of fraud is shown while the detection time increases or when fraudulent actors increase in number. In addition to visualising individual effects of some particular fraud, it should also be possible to visualise the correlations of misuse scenarios within a TSP service that make up fraud. Mostly, fraud is committed either through disguising as legitimate users or through leveraging legitimate services. Thus, the approach should clearly depict accepted scenarios, hidden transactions that could possibly happen between fraudulent actors, and potentially unwanted fraud scenarios in a given TSP service.

The evaluation criterion of these requirements is *usability*. The following are the high-level requirements on the visualisation component. In general the visualisation component should visualise:

- the contextual model, the impact of fraud and the correlations of misuse scenarios;
- fraud scenarios of a given TSP service.

6.5 Requirements on Data Management

The core targets of the fraud risk modelling approach are TSPs and similar service providers. A TSP has a lot of usage data of subscribers available for analysis, but their availability for processing may be legally restricted for e.g. data protection reasons. Thus, the fraud risk modelling approach should consider data management requirements.

The approach needs to provide performance scalability in order to be able to cope with massive amounts of data if needed, e.g. billions of CDRs. It should also be flexible to process data coming from different data formats as data sources stem from the domain of the different Telecom partners. The following summarises the requirements on the data management component. It should:

- be scalable to handle huge amounts of Telecom data. Evaluation criterion: *Scalability*;
- handle different data formats. Evaluation criterion: *Usability*.

7 Conclusion and Future Work

Fraud risks emerge due to single or combined individual risks against weakly protected elements of a service. Fraud risk modelling helps to identify weaknesses in the elements of the service, analyse the potential individual risks and estimate their impacts to the service provider. Even though the requirements are elicited from a limited number of fraud cases, they provide a *guideline* to develop a context-aware and usable fraud risk modelling approach besides improving the state-of-the-art on fraud risk assessment. One way of developing such an approach is by realising the requirements and apply the resulting approach to a list of Telecom services one by one and iteratively improve the approach in each development milestone. In this regard, the involvement of service providers is undoubtedly important in the evaluation of the approach.

In future, we plan to use the requirements above to develop a context-aware fraud risk modelling approach and refine it repeatedly based on feedback from Telecom providers, so that the approach can be applicable to one or several types of Telecom frauds. The other future research direction is to find detailed criteria to evaluate the effectiveness and usefulness of the fraud risk modelling approach.

References

1. CFCA.: Global telecom fraud report. Technical report, Communications Fraud Control Association (2015)
2. Yesuf, A.S.: A Review of Risk Identification Approaches in the Telecommunication Domain. In: Third International Conference on Information Systems Security and Privacy (ICISSP). (2017)
3. Farvaresh, H., Sepehri, M.M.: Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. In: Expert Systems with Applications. vol. 31, pp. 337–344. Elsevier (2006)
4. Estévez, P.A., Held, C.M., Perez, C.A.: A data mining framework for detecting subscription fraud in telecommunication. In: Engineering Applications of Artificial Intelligence. vol. 24, pp. 182–194. Elsevier (2011)

5. ISO/IEC, J.: ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management (2011)
6. TM Forum.: Enhanced Telecom Operations Map ® (eTOM) The Business Process Framework. (2015)
7. Macia-Fernandez, G., Garcia-Teodoro, P., Diaz-Verdejo, J.: Fraud in roaming scenarios: an overview. In: IEEE Wireless Communications. vol. 16. IEEE (2009)
8. Yufeng, K.Y., Chang-Tien, C.T., Sirwongwattana, S. and Yo-Ping,H.Y.: Survey of fraud detection techniques. In: IEEE International Conference on Networking, Sensing and Control. IEEE (2004)
9. Burge, P., Shawe-Taylor, J.: An unsupervised neural network approach to profiling the behavior of mobile phone users for use in fraud detection. In: Journal of parallel and distributed computing. vol. 61, pp. 915–925. Elsevier (2001)
10. Corporation, T.I.R.: The 2015 Telecommunications Industry Review: An Anthology of Market Facts and Forecasts. Technical report, The Insight Research Corporation (2015)
11. Cortesão, L., Martins, F., Rosa, A., Carvalho, P.: Fraud management systems in telecommunications: a practical approach. In: Proceeding of ICT. (2005)
12. Hilas, C.S., Mastorocostas, P.A.: An application of supervised and unsupervised learning approaches to telecommunications fraud detection. In: Knowledge-Based Systems. vol. 21, pp. 721–726. Elsevier (2008)
13. Jürjens, J., Schreck, J., Bartmann, P.: Model-based security analysis for mobile communications. In: Proceedings of the 30th international conference on Software engineering, 683–692. ACM (2008)
14. Gosset P., Mark, H.: Classification, detection and prosecution of fraud in mobile networks. Proceedings of ACTS mobile summit, Sorrento, Italy (1999)
15. The Smartvox Knowledgebase, http://kb.smartvox.co.uk/asterisk/secure-asterisk-pbx-part-1/, last accessed on Dec. 2016
16. Kuhn, D.R.: PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does. US Department of Commerce, Technology Administration, National Institute of Standards and Technology (2001)
17. Yelland, M.: Fraud in mobile networks. Computer Fraud & Security (2013)
18. Zuccato, A., Endersz, V., Daniels, N.: Security requirement engineering at a Telecom provider. In: Third International Conference on Availability, Reliability and Security (ARES), pp. 1139–1147. IEEE (2008)
19. Zuccato, A., Daniels, N., Jampathom, C.: Service security requirement profiles for telecom: how software engineers may tackle security. In: Sixth International Conference on Availability, Reliability and Security (ARES), pp. 521–526. IEEE (2011)
20. Qi, M.T., Xiao, Y.C., Jin, L.P., Ying, C.: Asset-based requirement analysis in telecom service delivery platform domain. In: IEEE/IFIP Network Operations and Management Symposium: Pervasive Management for Ubiquitous Networks and Services, pp. 815–818. IEEE (2008)
21. Krogstie, J.: Requirement engineering for mobile information systems. In: Proceedings of International Workshop on Requirements Engineering: Foundation for Software Quality (Interlaken, Switzerland). (2001)
22. Ionita, D., Gordijn, J., Yesuf, A.S., Wieringa, R.: Value-driven risk analysis of coordination models. In: IFIP Working Conference on The Practice of Enterprise Modeling. 102–116. Springer (2016)