Using Fraud Patterns for Fraud Risk Assessment of E-services

Ahmed Seid Yesuf, Jetzabel Serna-Olvera, Kai Rannenberg

Using Fraud Patterns for Fraud Risk Assessment of E-services

Ahmed Seid Yesuf, Jetzabel Serna-Olvera and Kai Rannenberg

Deutsche Telekom Chair of Mobile Business & Multilateral Security,
Goethe University Frankfurt, Frankfurt am Main, Germany
{ahmed.yesuf,jetzabel.serna,kai.rannenberg}@m-chair.de
www.m-chair.de

Abstract. Every year, e-service providers report losses of billions of dollars due to fraud. Despite their huge efforts in implementing sophisticated fraud detection systems on top of their e-services, fraud effects seem to be rather increasing than decreasing. As a result, *fraud risk assessment* has been introduced as a fundamental part of e-service providers' prevention strategies. In particular, identifying potential fraud risks and estimating their impacts are two essential requirements to prevent fraud risks while developing and delivering e-services to customers. In this paper, we show that *fraud patterns* can be used to perform fraud risk assessment. We analysed real fraud incidents from an e-service domain – Telecom, and identified six fraud patterns, which are recurrently used to commit fraud. We then use those patterns in the same scenario in order to demonstrate their applicability to fraud risk assessment.

Keywords: Fraud Pattern, Risk Assessment, Security, Fraud, E-service

1 Introduction

Over the past years, security and risk assessment have become essential requirements in the successful development of information systems and electronic services of enterprises [1]. In particular, since e-services (e.g. Internet marketing, telecommunication services and banking services) are delivered using technological means, it is of utmost importance to perform risk assessment in order to minimise or even prevent risks. One of the most relevant forms of risks which prevail in a wide range of e-service domains is fraud risk [2]. Fraud risk is a complex combination of social, financial and technological risks including misuses resulting from the flaws and weaknesses of e-services themselves. Therefore, preventing fraud is extremely relevant, since fraud negatively affects the global e-service revenue; for instance, in 2015, fraud affected the global Telecom revenue by almost $38.1 billion (USD) [3]. Thus, risk assessment is essential not only to counter fraud but also to keep e-services profitable and secured [4, 5].

Typically, frauds are perpetrated by individuals, organised groups of individuals, employees or third parties with a set of goals targeting the weak parts of e-services [6]. For an individual who has a service contract with a service provider

and uses it for individual purposes, the goal of perpetrating fraud is limited to individual benefit (e.g. using the service without/little payment). Beyond the individual benefit, organised fraudsters can potentially disrupt the business process of an enterprise (e.g. by colluding with third parties). In order to achieve their goals, they target customers, infrastructures of service providers (e.g. Private Branch Exchange – PBX systems), the service or product itself (e.g. service plan, credit card) and the entities involved in the process of delivering the e-services.

Until recently, a number of researches has focused on fraud detection methods such as [7–9]. In [2] and [6], authors present an extensive review and comparison of fraud detection approaches. Contrary to the many approaches which exist in fraud detection, fraud risk assessment has not been the target of many works. Authors in [10] and [11] have focused on fraud risk assessment. They proposed a value-based approach which can be used to identify and prioritise frauds, in particular, those occurring due to collusion with third parties. Although authors identified and focused on one of the most recurrent patterns that fraudsters use, they pointed out the need of performing fraud risk assessment with other types of fraud patterns in order to strengthen the security of e-services.

Considering that and given the wide range of methods and techniques to perpetrate fraud in e-services, fraudsters are able to use common but interchangeable patterns to achieve their goals. Thus, in this paper, we identify six fraud patterns from an e-service domain – the Telecom services. We therefore demonstrate how fraud patterns could be used to perform risk assessment of e-services and serve as a tool for preventing fraud risks.

The rest of the paper is organised as follows. Section 2 highlights concepts of fraud, e-services and fraud assessment in e-service. Section 3 presents the main methodology followed to produce the fraud patterns and use them towards fraud risk assessment. Section 4 describes the fraud domain model used to ease the interpretation of frauds. Section 5 presents an overview of the fraud incidents observed to identify the fraud patterns. Section 6 presents the identified fraud patterns followed by the application of the fraud patterns in a given scenario, namely Telecom services, which is then introduced in Section 7. Section 8 discusses the main advantages of this approach and highlights the open challenges and the limitations of the proposed approach; followed by the main conclusions of this paper in Section 9.

2 Background

2.1 Fraud risk in e-services

Fraud has several meanings that depend on the contexts. According to the Fraud Advisory Panel (www.fraudadvisorypanel.org), an anti-fraud community based in England, “fraud is the deliberate use of deception or dishonesty to deprive, disadvantage or cause loss (usually financial) to another person or party”. While this definition can be applied to a wide extent of auditing fraud, the Communication Fraud Control Association (CFCA) [3] has defined fraud as “the use of

telecommunication services or products with no intention of payment". Therefore, fraud risks in e-services are understood as events that allow fraudsters to misuse the service either to gain personal benefit or to the benefit of organised fraudsters. In this paper, we focus and explore those fraud risks that have impact on the service providers from the perspective of fraudsters.

2.2 Fraud Risk Assessment

Based on ISO 31000 [12], the risk management process includes five processes: establish context, risk assessment, risk treatment, monitoring and review, and communication and consulting. Risk assessment is an integral part of the risk management process, which is the concept of managing risks against enterprise objectives. More specifically, fraud risk assessment (FRA) is defined as the process of identifying, analysing and estimating fraud risks in a service.

Considering the impact of fraud on service providers, it is essential to prevent, detect and prepare the appropriate counter-measures. There exist a number of different approaches for fraud detection [6] [2]; however, preventing fraud through identifying and analysing business processes, transaction flows and other entities, still lacks the focus of the research community [4].

2.3 Fraud Patterns

The concept of patterns for security was initially introduced by Yoder and Barcalow [13]. The authors proposed seven security patterns that software developers should consider when developing their software applications. Since then, different types of security patterns were proposed (e.g. patterns for cryptography and access control [14]). "A security pattern describes a particular recurring security problem that arises in specific contexts, and presents a well-demonstrated generic solution for it" [15]. As such, the use of patterns has benefited security in several areas including software development. Inspired by this concept, we developed fraud patterns from the recurring fraud risks in the e-service domain. Fraud patterns not only help to describe recurring fraud risks in e-services but increase the potential of having in place preventive solutions. As a first step we have focused on the identification of the most relevant fraud risks.

3 Methodology

The whole process of a service provider from services delivery to the service payment process can be considered as a system. In such systems, one of the main challenges that directly or indirectly affect the revenue of service providers is fraud. Fraud risks are enabled when the weaknesses of the valuable assets (including their service) of service providers are exploited by fraudsters. Fraud risk assessment (FRA) is an approach to reduce the effects of fraud risks substantially – which is the goal of service providers. To develop a FRA approach, it is necessary to first develop a domain model or ontology of concepts related

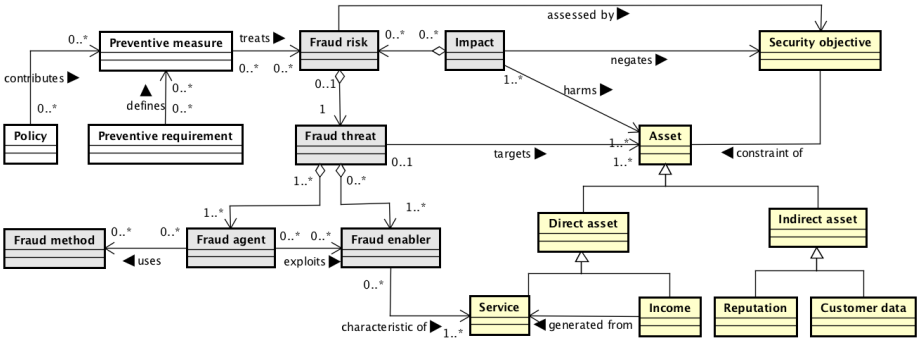

Fig. 1. Domain model for FRA (Fraud Risk Assessment): From left to right – *concepts of preventive measures, concepts of fraud and concepts of assets*

to fraud risks of such systems. Thus, we first adopted and extended the model introduced by [16]. By extending this model, we were able to develop a domain model specific for FRA. The domain modelling allowed us to better describe fraud risks in a particular domain. We considered the Telecom domain, and analysed five real fraud incidents in this domain. The analysed fraud incidents are business-related and are the result of different types of Telecom services (e.g., voice, PBX, roaming and Internet services). To develop the patterns, we applied the FRA domain modelling and interpreted the real fraud incidents. We identified six recurring and relevant patterns currently used by most fraudsters and actually present in more than one fraud incident. Finally, the applicability of the identified patterns is demonstrated by modelling the entities involved in the use case (Telecom domain scenario) and directly applying the fraud patterns to the model.

4 Fraud Risk Assessment Domain Model

In Information Systems Security Risk Management (ISSRM) [16] there exist different concepts that can easily be interpreted as concepts of FRA. The three groups of concepts mentioned in ISSRM – risk-based, asset-based and treatment-based concepts – could be adapted to the FRA domain model into concepts of fraud, assets and preventive measures. Based on this model, we defined a FRA domain model as shown in Fig. 1.

Concepts related to fraud

- *Fraud enabler* – is the potential weakness or possibility that enables a fraud to happen when exploited by a fraud agent.
- *Fraud agent* – is a fraudster or attacker who acts as an agent to perpetrate the fraud. A fraud agent uses fraud method and exploits fraud enablers.
- *Fraud method* – is an approach that a fraud agent follows to perpetrate the fraud.

- *Fraud threat* – is the combination of fraud agent and one or more fraud enablers. It targets one or more assets and its frequency/likelihood contribute for a fraud risk to happen.
- *Fraud risk* – is the combination of a fraud threat with one or more fraud enablers which negatively impacts one or more of the assets – direct or indirect assets.
- *Impact* – the negative effect of a fraud risk that harms one or more of the assets of the service provider. The impact on service provider can be interpreted in terms of money or reputation, by which both affect the revenue of the service provider.

Concepts related to assets

- An *asset* is any valuable entity of a service provider which could be targeted by one or more fraud agents (attackers/fraudsters); assets can be direct or indirect.
  – *Direct Assets* can be directly estimated when affected by fraud; they include *income* of a service provider or revenue/income for a given *service* (e.g. call, messaging, data, Internet services) by a service provider.
  – *Indirect Assets* cannot be directly estimated when affected by fraud; they include reputation and customer data.
- *Security objective* – is the protection measure that is applied to one or more assets. From the perspective of service providers, the security objectives include protection of direct and indirect assets including confidentiality, integrity and availability of services, prevention of service misuses and customer data protection (privacy).

Concepts related to preventive measures

- *Preventive measure* – is a part of fraud risk management; it is not part of a FRA. We include it into the domain model as it contributes to show the importance of FRA (e.g. preventive requirement specification based on FRA). It describes the treatment approach to a given fraud risk. This can be achieved by:
  – producing a *prevention requirement* – potential prevention requirements that need to be implemented in the system to protect the assets of the service provider, and/or
  – producing a new or modified *policy* – which is designed based on the assessment results of FRA. It could be enforced at the service level, organisational level, or customer level.

5 Modelling the Telecom e-services domain

The FRA domain model is applicable to different types of e-service domains (e.g. health insurance, Internet marketing, Telecom), where fraud is part of the risks of the respective services. In this paper, we considered the Telecom domain. In this domain customers subscribe to Telecom services. In the process of delivering the services, the Telecom providers are suffering from different types of frauds leading to important revenue loss [17] [3] [18].

Table 1. Fraud case 3. Stealing credentials to make unauthorised calls from a PBX (Private Branch Exchange) system

Description	A fraudster is able to retrieve a victim's telephony credentials from a PBX and sets up a call divert to a destination number of his choice for the victim's phone number. The fraudster then activates call forwarding to other Telecom destinations – mostly located abroad. The fraudster then makes the highest number of possible parallel calls through the diverted phone number. Calls or forwards triggered by the attacker are billed on a per-minute-basis to the victim's postpaid account. The destination Telecom passes a share of the received call-termination fees to the fraudster, thereby providing a payout per minute for incoming calls as incentive to generate as much incoming traffic as possible to the Telecom network.
Fraud enabler	– Vulnerabilities of the PBX – Weak configuration of policies at PBX (e.g. remote access to the PBX) – The availability of Telecom providers that could pay out the income share to the fraud agents who can manage to generate a lot of call traffic to customers of those Telecoms.
Fraud agent	A fraudster who is an outsider
Fraud method	Call forwarding, social engineering, impersonation
Fraud threat	Revenue share
Asset	Credentials and income of the service provider
Security objective	Confidentiality of credentials and misuse protection
Fraud risk	– A bill with high cost to the customers – The customer might not pay the bill.
Impact	Financial damage and service disruption (unavailability)
Preventive measure	– Implementation of strong PBX policies – Create awareness of social engineering to the customer – PBX maintenance

5.1 Fraud scenarios

Due to space limitation, we briefly describe the five scenarios spanning different types of real frauds. In the next subsection we further focus on two of the most relevant frauds, which are then interpreted using the domain model in Tables 1 and 2.

Fraud case 1.
Name: Service plan misuse with the involvement of a third party
Target: Income of the targeted Telecom service provider
Goal: To gain financial benefit and use the service without payment.

Fraud case 2.
Name: Identity theft to use the call-forwarding functionality of (a) post-paid contract(s)
Target: Income of the targeted Telecom service provider
Goal: Call selling, using service without payment

Table 2. Fraud case 4. abusing fixed line network credentials during service set-up process of an Internet access service (DSL connection)

Description	A fraudster orders a land-line Internet connection with a Telecom provider. In doing so, he uses fake customer data. An order confirmation will be sent to the fraudster's address, stating a service connection date. Sometime before a technician visits the place, fixed line network credentials will be sent via letter to the fraudster. The fraudster takes the credential letter as soon as it arrives and uses the respective credentials for SIP authentication, logging on to the TSPs telephony server from another location (securing its anonymity).
Fraud enabler	– Poor identity check – Service availability before the necessary devices are installed
Fraud agent	A fraudster who pretends to be a real customer
Fraud method	– Exploiting poor identity checks – Exploiting the time interval before the service charge is recorded
Fraud threat	Call selling, service distortion and social engineering of service provider
Asset	Income of the service provider
Security objective	Misuse protection
Fraud risk	Impersonation of customers and scamming the service provider
Impact	Financial damage
Preventive measure	– The message conversations between the customer and the service provider should be certified. – Start the service once the apparatus is configured – The credentials must be sent only to legal user with certified identify.

Fraud case 3.
Name: Stealing credentials to make unauthorised calls from a PBX system
Target: Credentials of the PBX system and income of the Telecom service provider
Goal: Financial gain (e.g. by call selling) and using service without payment

Fraud case 4.
Name: Abusing fixed line network credentials during service set-up process of an Internet access service
Target: Income of the Telecom service provider
Goal: Using service without payment

Fraud case 5.
Name: Service plan misuse to perform roaming fraud
Target: Income of the Telecom service provider
Goal: To gain financial benefit

5.2 Fraud pattern development

In order to identify the fraud patterns, we modelled the Telecom domain using the five aforementioned scenarios. We have interpreted these frauds using the fraud domain model developed in Section 4. Tables 1 and 2 show the modeling of two of the five scenarios. Note that the goals of fraudsters are diverse, but we only focused on those which have an important effect to the Telecom service provider.

6 Fraud Risk Patterns (FRPs)

Fraud risk patterns (FRPs) are similar to security patterns described in [15] [19], which describe a particular recurring *security* problem that arises in specific contexts, and present a well-proven generic solution for it. In our context, we are interested in recurring *fraud risks* against the valuable assets of service providers.

After defining each of the five fraud incidents using the FRA domain model (cf. Section 4), we have observed each of the fraud cases and found a list of recurring fraud enablers targeting the assets of the Telecom (e.g. the service itself and the income). Fraud agents (fraudsters) have different goals in perpetrating a fraud, most of them target the Telecom service to gain a lot of money – which indirectly affects the income of the Telecom for that specific service. Each of the fraud cases has security objectives and can mainly be categorised into three security objectives: misuse protection, CIA (confidentiality, integrity and availability) and privacy (data protection). In the process, we produced three groups of FRPs: patterns related to service-misusing, patterns due to system vulnerabilities and patterns related to privacy (data protection). In this paper, we are interested analysing the first two groups of patterns. The FRPs identified below are distributed across the five fraud cases.

Patterns related to *service-misusing*

FRP 1 – Impersonation (of customers or service providers):

Context. This describes a situation where a fraudster pretends as a legal customer or a representative from a service provider to achieve his/her goal. In the *Fraud case 3*, for instance, the fraudster provides wrong information about his personal information including the address to impersonate a legal customer in order to get credentials necessary to commit the fraud. Beyond this, the fraudster can have a different approach to get the credentials by impersonating the technician of the service provider to get the credentials from a legal customer.

Target. This pattern targets customers and service providers. It is observed in the *Fraud cases 3,4* and *2*.

FRP 2 – Time interval-based misuses:

Context. In this pattern, the fraud is perpetrated following the availability of a service without the knowledge of the service provider or in a condition where the service provider could not recover the damage caused by the fraud. In *Fraud case 4* (see Table 2), for instance, the service provider sends the call credentials before the necessary infrastructure is configured at the customer place, while

the service is activated and available to be used. In the case of VoiP telephony, the credentials are enough to set up a remote connection and perform the fraud. Obviously the main fraud enabler is the availability of the service before it is accountable to the customer. Note: This kind of fraud could also be exploited by a third party – stealing the credentials, in which case it follows FRP1.
Target. The target of this pattern is generally time-dependent activities. It is observed in the *Fraud cases 4* and *5*.

FRP 3 – Misusing the service by overdoing beyond the expected limit:
Context. In this pattern, a fraudster uses the service beyond the expected usage limit of "normal" customers. For example, in a service plan misuse case, a fraudster tries to generate a lot of call traffic while keeping himself undetected by the fraud detection system installed at the service provider side. This is a very common fraud that a Telecom service provider is facing, which needs careful service planning.
Target. The target of this pattern is the service and its tariff plan. We observed this kind of fraud pattern in all of the *Fraud cases 1 to 5*.

FRP 4 – Fraud due to invisible collusions:
Context. In this pattern, a fraudster perpetrated the fraud in an organised entity where other customers or service providers are involved directly or indirectly to gain financial benefit. A rational fraudster uses all possible ways of getting the benefit from the service either by installing a PBX system that helps to sell calls or randomly generating calls to expensive destination. In this case, the fraudster will make an agreement with a third party (mostly another Telecom service provider) to terminate calls to expensive destinations. In return, the fraudster gets his income share generated by committing the fraud with the third party.
Target. This pattern targets the service providers and the weaknesses on their services. It is observed in the *Fraud cases 1, 2* and *5*.

Patterns due to *vulnerabilities of the system*

FRP 5: Unsecured (uncertified) communication
Context. This describes a fraud pattern due to lack of secure communication between different business entities in a given context. For instance, when a user has a possibility to register as a new customer via the Internet, the user might use a forged identity and delivery address unless the system implements a way of user certification. This allows fraudsters to trigger the process of creating a contract or an account to gain the advantages that a forged identity can get.
Target. This pattern targets the communication channel between entities in the e-service. It is observed in the *Fraud case 4*.

FRP 6: Exploiting infrastructure vulnerabilities:
Context. This is a situation where technical weaknesses of the infrastructure at a service provider or at a customer point contribute to a fraud. In *Fraud case 3*, for instance, a weak configuration of the remote access policy of the PBX system is the main triggering factor for fraudsters to target the PBX.
Target. This fraud pattern targets the infrastructures used to deliver the e-services. It is observed in the *Fraud cases 3* and *4*.

7 Application of FRPs to Telecom Services

So far, we have presented fraud patterns identified from the real fraud incidents. In this section, we use an e-service from the Telecom domain, namely the *roaming service*, to apply the fraud patterns and show how they could be used for fraud risk assessment. To do the fraud risk assessment, first the necessary entities need to be described. Then, for each fraud pattern, the potential fraud risks would be identified. At last, the potential fraud risks should be estimated based on their impact on the service provider.

7.1 Case study description

Roaming is one of the Telecom services which allows customers to use calling and messaging services while they are abroad. It involves different independent actors: the customer, the visited and the home service provider. We focus on the calling service of roaming for the sake of simplicity.

The customer. A customer creates a contract (either flat-rate or pre-paid) with the home service provider to get call services – roaming. He is responsible to pay for the services he has used.

The home service provider (HSP). A HSP is responsible for providing calling services to their customers within the coverage of customers' contract. The HSP maintains the usage data of customers including access locations in a database – home location register (HLR). To prepare the invoice for the roaming service of a customer, the HSP should receive call detail records (CDR) from the visited service provider. The CDR is the usage data of a customer stored in the visited service provider. The payment for the roaming service is based on the number of minutes that the customer calls while roaming.

The visited service provider (VSP). A VSP will have a roaming service *agreement* with the HSP to provide roaming service to the customers of the HSP when the customers use the service within the VSP network. The VSP is responsible for storing and sending the CDRs of the customer to the HSP. Based on technologies implemented at the VSP, the reporting time varies. According to the technology Near-Real-Time Roaming Data Exchange (NRTRDE), the time to report is limited only to four hours.

Entities in the case study

The e-service under assessment can be represented in a structural model, which represents the necessary entities for the assessment. Each of the fraud pattern targets a specific set of e-service entities such as actors, activities, services, communication channels and infrastructures. Finding a suitable modelling language to handle all types of e-service entities is a future work. An example model to represent the relations between actors in a semi-structured model is shown Fig. 2.

- ***Actors.*** *Customer* (type: human), *HSP* (type: service provider), and *VSP* (type: service provider). The actor *HSP* can be expressed with its employees such as customer services, technicians and commercial managers.

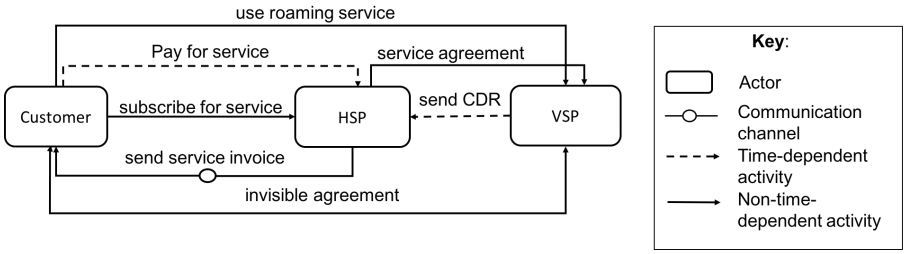

Fig. 2. A semi-structured model for the roaming service case

- ***Activities.***
  - *Time-dependent activities. VSP* sends CDR file of customer to *HSP* within certain time interval; A flat-rate roaming customer pays every month for the service he used;
  - *Non-time-dependent activities. Customer* creates contract or subscribes to a service; The HSP has roaming service agreement with the VSP; the *customer* is able to *use* the roaming service while being in the *VSP*'s network, and maybe creates an agreement with VSP to commit fraud (i.e., invisible to the HSP).
- ***Services.***
  - *Assets.* The roaming service (type: service); the payment (type: income)
  - *Service usage limit.* Contracts between *customer* and provider (for pre-paid contracts – the customer can use as long as the account balance is above zero, for flat-rate contracts – mostly the customer has yearly contracts payable monthly); between *HSP* and *VSP* (payment for the services that the customer of the *HSP* gets – paid per number-of-minutes of calls)
- ***Communication channels.*** At the time of the contract creation, the communication between the customer and the HSP is either through letters, emails, on-line registration or personally at the customer service. File transfer from VSP to HSP is through encrypted channel between the two.
- ***Infrastructures.*** *HSP* database and *VSP* database systems (type: NRTRDE or other)

7.2 Risk assessment

Fraud risk assessment is the process of describing the e-service under assessment, analysing fraud risks and estimating their impacts. The goal of risk analysis is to identify the potential fraud enabling factors using FRPs. To achieve this goal, we have to check all the fraud patterns against the service described above; due to space limitation, we only show this for FRP1 and FRP2. Each fraud pattern targets different entities in the e-service. A strategy of identifying the potential fraud enabling factors is by asking questions whether each FRP enables fraud targeting entities in the given e-service.

To estimate the potential impact to the HSP, we can use a qualitative measurement: *high*, *medium* and *low*. *High* is when the impact of the fraud is substantial to the HSP that they lose a lot of money beyond the expected expenses. *Low* is when the impact of fraud is within the customer's contract limit though has an effect on the income of the HSP. *Medium* is between the scale *high* and *low*. For each example fraud identified, we provide high level preventive measures in terms of security requirements.

FRP1 – impersonation. As the target of FRP1 is customers and service providers, and the goal of fraudsters in this fraud pattern is to gain financial benefit or use the service without payment, the question should be: *how could customer and HSP possibly be impersonated in the roaming case so that fraudsters gain financial benefit or use the service without payment?* Here are some examples:

1. A fraudster could impersonate the customer-service of the HSP to create a flat-rate roaming contract. The fraudster can then generate calls at least for a month until the service is interrupted.
   – *Impact. High* as the service provider is the main target by the fraudster.
   – *Preventive measures.* 1) Strong identity check (e.g. credit check with authorised third party) 2) train the personnel at customer-services about the threats of impersonation;
2. A customer who has a flat-rate roaming contract could be impersonated to clone his SIM-card or to lose his device as it allows a fraudster to commit fraud until the fraud detection system detects it or a customer informs the HSP to stop the service.
   – *Impact. Medium* because the customer is the main target affected by the fraudster, so enforced to pay. In the cases where the customers did not realise the fraud and did not report to the HSP or the fraud detection system didn't detect, the effect might go beyond the customer to affect the income of HSP.
   – *Preventive measures.* 1) Inform the customers who have contracts with the HSP about the common fraud patterns that they might be suspicious 2) advance the fraud detection mechanism to handle SIM cloning and similar impersonation techniques;
3. A fraudster creates a roaming service contract via the HSP's online registration portal with fake identity and credit information.
   – *Impact. High* because the fraudster could resell the service until identified and this directly affects the HSP.
   – *Preventive measure.* The registration portal should certify users and check their credit.

FRP2 – time interval-based misuse. The targets of FRP2 are time-dependent activities. So, the question should be: *How would time-dependent activities be used to misuse the service?* Here are some examples:

1. Because of the time-delay before the VSP sends the CDRs of a customer, fraudster could use the roaming service to call to an expensive destination

without being detected or the service being interrupted. This is mainly dangerous if the fraud detection technology is weak at the VSP side.
– *Impact. High* because 1) there is an unpaid bill by the fraudster and 2) the HSP has to pay the termination fee (for the calls terminated in the VSP network).
– *Preventive measures.* 1) Limit the amount of time taken to send the CDRs of customers from VHP to HSP 2) Install standardised technologies with both HSP and VSP to prevent modification of CDRs – sometimes this is difficult to implement at VSPs due to lack of jurisdiction).

2. When a fraudster manages to get a flat-rate roaming service, the time-limit to pay the monthly service charge is in danger.
– *Impact. High* because flat-rate services mostly have no usage limitation which leaves the HSP with the unpaid bill.
– *Preventive measure.* The HSP should ensure that the customer has not been involved in a fraudulent behaviour (e.g. with the help of credit check organisations).

8 Discussion

Fraud patterns can successfully be applied not only in the process of FRA, but as well as for producing security requirements and policies. One of the main benefits relies on the fact the each of the fraud patterns targets a specific entity within the e-service model. The description of e-services (e.g. using appropriate modelling languages) thus plays an important role in using them for risk assessment. Since fraud patterns have been identified from five recurring fraud incidents in Telecom e-services, it would be valuable to perform the validation and improvement of those with real practices. Furthermore, the applicability of fraud patterns has only been shown in one domain; other e-services and domains would be interesting for demonstrating the applicability of fraud patterns in FRA of e-services in general. Note, that while performing FRA of e-services allowed us to identify fraud risks, it is also important to put fraud detection approaches in place to gain the full advantages of fraud management.

9 Conclusion and Future Work

Fraud pattern is a handy way of identifying fraud risks from the perspective of fraudsters. They are an essential part of fraud risk assessment to ease the task of fraud managers to put their preventive measures in place before the fraudsters damage the assets (directly or indirectly). This also increases the security and profitability of e-service providers.

Even though the fraud patterns identified in this paper are from a limited set of existing frauds, they are important to guide future development on fraud patterns. Therefore, to enhance the fraud patterns, we plan to develop a fraud risk assessment tool and apply the fraud patterns for different e-service domains beyond the Telecom domain.

References

1. 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, IEEE (2011)
2. Rebahi, Y., Nassar, M., Magedanz, T., Festor, O.: A survey on fraud and service misuse in voice over ip (voip) networks. Information Security Technical Report **16**(1) (2011) 12–19
3. CFCA: Global telecom fraud report. Technical report, Communications Fraud Control Association (2000-2015)
4. Yesuf, A.S.: A Review of Risk Identification Approaches in the Telecommunication Domain. In: The 3rd International Conference on Information Systems Security and Privacy, ICISSP. (2017)
5. Yesuf, A.S., Wolos, L., Rannenberg, K.: Fraud Risk Modelling: Requirements Elicitation in the Case of Telecom Services. In: The 8th International Conference on Exploring Service Science, IESS 1.7. (2017)
6. Abdallah, A., Maarof, M.A., Zainal, A.: Fraud detection system: A survey. Journal of Network and Computer Applications **68** (2016) 90–113
7. Hilas, C.S., Mastorocostas, P.A.: An application of supervised and unsupervised learning approaches to telecommunications fraud detection. Knowledge-Based Systems **21**(7) (2008) 721–726
8. Ruiz-Agundez, I., Penya, Y.K., Bringas, P.G.: Fraud detection for voice over ip services on next-generation networks. In: IFIP International Workshop on Information Security Theory and Practices, Springer (2010) 199–212
9. Farvaresh, H., Sepehri, M.M.: A data mining framework for detecting subscription fraud in telecommunication. Engineering Applications of Artificial Intelligence **24**(1) (2011) 182–194
10. Ionita, D., Wieringa, R.J., Wolos, L., Gordijn, J., Pieters, W.: Using value models for business risk analysis in e-service networks. In: IFIP Working Conference on The Practice of Enterprise Modeling, Springer International Publishing (2015)
11. 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, Springer International Publishing (2016) 102–116
12. ISO/TC 262 Risk management: ISO 31000:2009, ISO 31000:2009 Risk Management – Principles and Guidelines (2009)
13. Yoder, J., Barcalow, J.: Architectural patterns for enabling application security. Urbana **51** (1998) 61801
14. Braga, A., Rubira, C., Dahab, R.: Tropyc: A pattern language for cryptographic software. (1999)
15. Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., Sommerlad, P.: Security Patterns: Integrating security and systems engineering. John Wiley & Sons (2013)
16. Dubois, É., Heymans, P., Mayer, N., Matulevičius, R.: A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Intentional Perspectives on Information Systems Engineering. Springer Berlin Heidelberg, Berlin, Heidelberg (2010) 289–306
17. Rosas, E., Analide, C.: Telecommunications fraud: Problem analysis-an agent-based kdd perspective. Aveiro: EPIA **2009** (2009)
18. Ghosh, M.: Telecoms fraud. Computer Fraud & Security **2010**(7) (2010) 14–17
19. Rrenja, A., Matulevičius, R.: Pattern-Based Security Requirements Derivation from Secure Tropos Models. Springer International Publishing (2015) 59–74