Estimating the Risk of Fraud against E-services

Ahmed Seid Yesuf[1]✉ and Christian W Probst[2]

[1] Deutsche Telekom Chair of Mobile Business and Multilateral Security
Goethe University Frankfurt
Frankfurt, Germany
ahmed.yesuf@m-chair.de
[2] High-Tech Transdisciplinary Research Network
Unitec Institute of Technology
Auckland, New Zealand
cprobst@unitec.ac.nz

Abstract. Industry is continuously developing, deploying, and maintaining e-services to transform traditional offerings. While protection of traditional services is well understood, their digital transformation often is vulnerable to known and new attacks. These vulnerabilities open the door for fraudsters to exploit the weaknesses of the new systems and associated services, causing losses of billions of dollars for global economy. This development is caused by the ease of developing new offerings, and the difficulty of performing thorough risk assessment during their design and development. Traditional risk assessment methodologies need to be enhanced to include threat scenarios faced by e-services, and to enable them to match the short development timeframes and to inform the decision-making process. In this paper we present a fraud risk estimation approach addresses these requirements. Based on a list of threat scenarios, our approach calculates the potential risk using pre-computed risk factors, and visualises the analysis result for an informed decision making. In doing so, our approach increases visibility and awareness of fraud risks, and reduces the time spent to calculate potential risks at the design level and throughout development. Together, these properties make our fraud risk estimation approach ideally suited for constantly applied, iterative risk analysis.

Keywords: risk estimation · risk analysis · e-service · fraud · security

1 Introduction

Electronic services or e-services are an umbrella concept for services in different areas utilising information and communication technologies, most prominently the Internet. They are different from non-electronic services by their characteristics of continuous improvement and deployment, transparent service feedback and rapid development [13]. Examples include e-Government and e-Health, but also traditional services are increasingly transformed into e-services across domains and industries in the process of streamlining operations and easing interaction with both existing and novel services of organisations. Not surprisingly,

the technological transformation in providing e-services has also led to a drastic increase of attacks and fraudulent activities by cyber criminals.

According to a report, attacks on e-services produce an estimated loss of $600 billion in 2017 alone [9]. One of the most important cyber crimes against e-services is fraud, that is the use of services with no intention of payment [3], and the misuse of services for individual or organised benefits [2]. Fraudulent attacks often exploit weaknesses at the social, technical, and economical layer [12]. This could be avoided if stringent risk assessment would be applied continuously when new or updated services are planned. However, the ease and speed of developing and deploying services today is diametrically opposed to the difficulty of performing risk analysis.

A number of different security risk assessment methods are designed to identify and analyse different types of risks at a system level [15]. While the application of these assessment methods generates a large number of threat scenarios, there are at least three problems analysing the risk they pose. First, current approaches collect information about the threat predominantly by brainstorming or doing expert interviews for further assessment [15]. This is often too time-consuming a process, but especially so for e-services, considering their characteristics and how little time it requires to release a new service to customers. Second, an informed decision must be based on a calculation of the potential risk based on relevant factors leading the threat scenario [8]. When these factors are unavailable, decisions must be made based on incomplete inputs, and thus will not be able to address potential risks against the service under assessment. Third, a large number of threat scenarios could produce a corresponding large number of risks to the service. The risks or their impact must be presented in a human-readable format to support decision makers have informed decisions, which requires tool support.

In this paper, we present *Fraud Risk Estimation* (FRE), an automated approach that addresses the issues identified above. Fraud Risk Estimation precalculates impact, likelihood, and consequently risks of threats based on different risk factors. The resulting risks are visualised, to enable analysts to understand and identify the largest risks and contributing factors. The calculations are performed for different risk factors depending on threat scenarios, and are visualised to support the decision-making process.

Our approach includes a novel method to address missing or unreliable values, which are notoriously difficult to account for in established methods. We introduce sliders inspired by tools for analysing MRI results, where doctors look for discontinuities in large sets of pictures instead of individual pictures. Sliders enable the analyst to quickly see the risks for differing values of variables and the risks these values lead too.

Compared to traditional approaches, our approach has the advantage of assessing the service in terms of expected risks, directing decision makers to the parts of a service that must be addressed to reduce the potential risks, and enabling continuous risk analysis throughout the development process.

The rest of the paper is organised as follows. After a discussion of related work in Section 2, we discuss the relevant definitions used to design FRE including threat scenarios, risk factors and risk metrics in Section 3. Then, Section 4 presents the proposed risk estimation approach, its architecture, the process of estimating risk, and algorithms. Section 5 presents the tool we developed for FRE, an application of the approach to a case study, and an experiment on the performance of the prototype. Section 6 discusses the advantages and weaknesses of the FRE approach, and Section 7 summarises the paper with concluding remarks and a discussion of future work.

2 Related Work

An important part of cybersecurity frameworks and standards is Security Risk Assessment (SRA). The NIST Cybersecurity framework [11] and ISO 27001 [7], for example, provide guidelines to SRAs and how to identify, analyse, and estimate security risks. They require design and implementation steps according to the type of risks a system or a service encounters. We discuss some exemplary approaches we thought have applicability for service domains in estimating fraud risks and compare them to our approach.

Structured Risk Analysis (SRA) is a method to help organisations take rational steps to improve their information security [10]. The approach calculates the actual risk from system vulnerabilities and service threats, and relies on user-defined qualitative risk metrics. While the process is described very clearly, the main concerns are the required user inputs and manual computation, and a lack of visualisation of results.

CORAS is another model-driven SRA [16] with guidelines and steps to perform the assessment [1]. CORAS has eight steps, four of them focussing on context-understanding, and the other four focussing on risk identification, estimation, evaluation, and risk treatment. A software tool represents the context visually, including unwanted incidents and possible treatments of the risks. Also CORAS relies on expert input to understand the context and the risk analysis steps, and the risk estimation relies solely on manual computation of risks, making it difficult to apply for iterative risk analysis with changing context information. This is especially relevant for e-services that are continuously developed and deployed.

Factor Analysis of Information Risks (FAIR) is yet another SRA that takes different risk factors into account [6]. It qualitatively estimates the impact of different variables, but it also relies on expert knowledge to estimate the risk.

In contrast to these approaches, our approach supports automated calculation and visualisation of risks to facilitate informed decision making, and an easy exploration of potential valuations of factors deemed relevant for a given scenarios, for example, the likelihood of success, the skill level of a fraud agent, etc. This is achieved through pre-computation of risk factors to estimate the potential risk, and through visualisation of analysis results. These factors are especially beneficial when expert inputs are incomplete.

Table 1. Concepts and Notations, all mutually exclusive.

Symbol	Definition
F_e	Fraud enabler
F_{agent}	Fraudster who acts as an agent
F_{threat}	A fraud threat i.e., combination of F_{agent} and F_e
T_{asset}	Targeted asset direct or indirect
F_{risk}	Combination of a F_{threat} and F_e that could affects T_{asset}
SL_i	Skill level of an entity i
$SecL_i$	Security level of an entity i

Symbol	Definition of Sets
A	Actors = $H \cup O$
B	Actions of actors
C	Communication media = $N \times \mathcal{R} \times N$
E	E-service connections and interactions
H	Human actors
I	Infrastructures
N	E-service nodes = $A \cup B \cup I \cup Y$
O	Organisational actors
Y	Assets (service, income, credential, money)
$\mathcal{R}$	Relations, *e.g.*, *agreement*, *partOf*, *possesses*, *communication*

Overall, FRE is not designed to substitute the risk assessment process of well-established SRAs, but complements them through automatic computation of risks from pre-computed likelihood values, visualising the analysis results to be understandable by decision makers and supporting iterative risk estimation when the context of threat agents and defenders is changing.

3 Baseline: Threat Scenarios and Risk Model

We now present our methodology motivated by the related work on risk analysis, specifically on risk estimation. We define the concept of threat scenarios in e-services and identify the factors or variables influencing fraud risk of e-services, followed by the risk metrics for impact and likelihood. Table 1 introduces some terms used throughout this paper.

3.1 Threat Scenarios in E-services

Models are widely used to represent software systems, business models, and services to enhance understanding and communication between different stakeholders [5]. An *e-service model* $em \subseteq N \times C$ describes the target of assessment (ToA) using nodes and interactions between nodes [17].

For instance, the IP-based Private Branch Exchange (IP-PBX) service we consider in Section 5 is an e-service in the Telecom industry that delivers call and data services using the Internet. IP-PBX switches Voice Over IP to public switching telephone network. The conceptual model of an IP-PBX system contains independent actors, infrastructure, assets, and different types of connections, some of which are shown in Table 2.

Table 2. Examples of nodes and connections in the IP-PBX case

Nodes	*actors* (Telecom operator, company, employees, administrators of IP-PBX), *infrastructure* (IP-PBX), *assets* (call, data, call forwarding service)
Connections	⟨company, agreement, *Telecom operator*⟩, ⟨employees, partOf, *company*⟩, ⟨company, possession, *call service*⟩, ⟨employees, communication, *IP-PBX*⟩

A *fraud agent* is a person or a group of organised actors who aim to gain a benefit by committing fraud. A *fraud enabler* is an entity with a potential weakness that enables a fraud to happen when exploited by a fraud agent. A *fraud threat* is the combination of a *fraud agent* and one or more *fraud enablers*. The threat targets an asset, and its likelihood contributes to the fraud to happen. These concepts are originally taken from Dubois *et al.* [4] and adopted for the context of e-service models [18]. In this paper, we assume the list of threat scenarios to be identified from the model using pattern-based risk identification [14, 18], an efficient technique to quickly assess threats in systems.

In e-service models, a fraud enabler is an actor, an action, an infrastructure, or a communication medium, a *fraud threat* F_{threat} is $(F_{agent}, F_{enabler}, T_{asset})$, with $F_{agent} \in A$, $F_{enabler} \in A \cup B \cup C \cup I$, and the target asset $T_{asset} \in Y \times [0,1] \times A$, which has an owner and a likelihood of success.

3.2 Risk Factors

Risk factors describe behaviours of entities in an e-service model, and capture the likelihood of a threat scenario to succeed and contribute to an actual risk. To estimate the risk of a threat scenario, we analyse fraud threat scenarios and the behaviours of model entities.

Skill level SL_i defines the capability of a fraud agent to exploit a fraud enabler, resulting in a risk, or of a defender to counter a possible threat. Depending on the actor, the skill level can be basic, intermediate, or high.

Noticeability is a property of an *action* to indicate whether a threat scenario can be identified immediately at the time when a fraudster commits it, and can be noticeable or unnoticeable. Time-dependent actions are noticeable within a certain time limit, but time-independent actions require additional effort from the defenders to be noticeable, otherwise it will stay unnoticeable. For example, paying a contract fee is a time-dependent action that is required to be paid with in a week or a month. This action is noticeable after a week or a month.

Security Level $SecL_i$ describes the level of protection from a threat for technical entities in the model, and can be secure, not secure, or unknown. For example, the communication between a customer and a service provider using an uncertified communication medium is *not secure*.

Resource estimates the required resources to commit a fraud or defend against it. In this paper, we assume resources to be constant and they play no role in risk estimation, but could easily be added as another value.

3.3 Risk Metrics

A risk is defined as $F_{risk} = impact \times likelihood$, leading to qualitative risk metrics for fraud against e-service assets. Assets can be direct like *service* and *income* generated by the service, or indirect, like *credentials* and *personal identities*.

The impact against direct assets is calculated based on the damage to that specific service in terms of *asset value*. The impact against indirect assets is calculated based on its contribution for the damage of direct assets. For example, when a credential has a direct relation to a direct asset, the asset value of the credential is the same as that of the asset. Otherwise, the contribution does not have impact to the direct asset. Based on asset value x and agreed amount$y$ of the overall asset value, we compute impact:

$$Impact(x,y) = \begin{cases} VeryHigh & \text{if } x \geq 4/5y \\ High & \text{if } 3/5y \leq x < 4/5y \\ Medium & \text{if } 2/5y \leq x < 3/5y \\ Low & \text{if } 1/5y \leq x < 2/5y \\ Negligible & \text{if } x < 1/5y \end{cases}$$

The likelihood of a fraud agent to succeed in exploiting a threat is calculated using the risk factors of fraudsters and defenders. These include the SL_f, SL_d, $SecL_i$, *noticeability*, and *resources*. Assuming that the required resources are constant, the likelihood varies depending on the target of the threat. For a threat $(a, e, (t, p, o))$ with fraud agent a, enabler e, and targeted asset t, likelihood of success p, and owner o, there are three cases to consider based on the enabler:

$$Likelihood((a, e, (t, p, o)), d) = \begin{cases} SL_{f \to d} & \text{if } e \in A \\ SL_{f \to d} * noticability & \text{if } e \in B \\ SL_{f \to d} * SecL_i & \text{if } e \in I \cup C \end{cases}$$

where $SL_{f \to d}$ is the skill level of fraudster F_{agent} against the skill level of the defender d, which can be an actor, infrastructure, or communication medium. If the enabler is an actor, the likelihood depends on $SL_{f \to d}$, which is computed by

$$SL_{f \to d} = \begin{cases} Likely & \text{if } SL_f > SL_d \\ Possible & \text{if } SL_f = SL_d \\ Unlikely & \text{if } SL_f < SL_d \end{cases}$$

If the enabler is an action, the likelihood depends also on the *noticeability*. Finally, if the enabler is an element of the infrastructure or communication media, the likelihood depends on both $SL_{f \to d}$ and the enabler's security level $SecL_e$:

$$SecL_e = \begin{cases} Likely & \text{if } e \text{ is not secure} \\ Possible & \text{if } e \text{ is not known} \\ Unlikely & \text{if } e \text{ is secure} \end{cases}$$

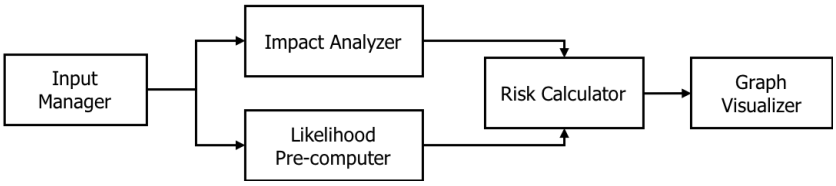

Fig. 1. The Fraud Risk Estimation architecture (the boxes indicate the framework components and the arrows indicate sequences.

4 The Fraud Risk Estimation Framework

The Fraud Risk Estimation framework (FRE) analyses the possibilities of threats against e-services to succeed, through computing the potential impact, calculating the overall risk, and visualising the analysis results. Together, these are the crucial elements to assess the huge number of threat scenarios an e-service may face, and to enable informed decision making. In this section, we present the FRE framework and the algorithms applied, as well as a prototype tool.

4.1 The FRE Architecture

The architecture of FRE enables risk estimation by pre-computing the possible variables for missing values. In other words, FRE automates the risk estimation process to enable informed decision making. The high-level architecture is shown in Figure 1. The process of FRE, as shown in Figure 2, is a three-stage process based on input management, risk calculation (impact and likelihood calculations), and the visualisation of the computed risks.

The input management provides the necessary data to perform the risk estimation as discussed in Section 3: an e-service model to assess, a list of identified threat scenarios, and risk factors. The list of fraud threats contains fraud agent, fraud enabler, and targeted asset, the risk factors indicate the possibility of a threat scenario to succeed in producing a potential risk (Section 3.2), and the e-service model is a description or representation of the system with nodes (human and organisational actors, actions and infrastructure and assets) and interactions (communications, payment transactions and value exchanges including the corresponding asset values), similar to those developed by Yesuf [17, 18].

Based on these inputs, the automated computation performs an impact analysis, likelihood computation, and risk calculation. The impact analyser computes the impact of a threat scenario based on the agreement between the service provider and the user, in which the user agrees to pay a certain amount of fee for the service (in this case the affected asset). Using the measure for impact described in the previous section, the impact analyser compares the asset value against the agreed asset value and produces an estimated impact, ranging from negligible to high impact, resulting in a list of threat scenarios and their impact value. In parallel, we pre-compute the likelihood of a threat scenario based on

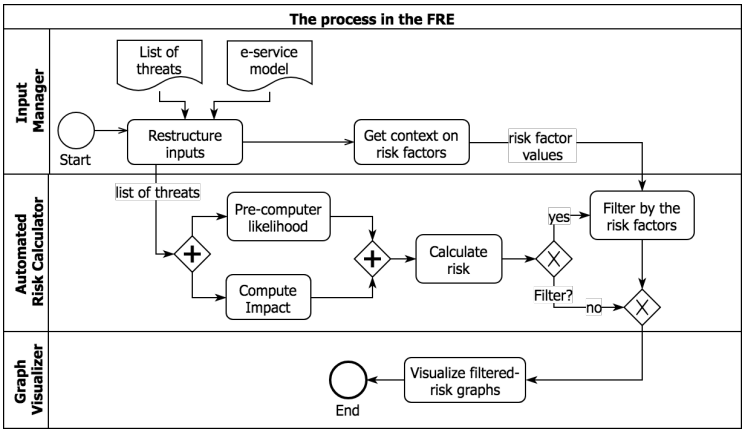

Fig. 2. The process in FRE.

Algorithm 1 Impact computation

procedure COMPUTEIMPACT(t, $maxT$) ▷ `Threat` t, `max threshold` $maxT$
  $assetValue \leftarrow t.getAssetValue$
  if $assetValue \geq 0.8 \cdot maxT$ **then**
    $impact \leftarrow 5$
  else if $assetValue \geq 0.6 \cdot maxT$ & $assetValue < 0.8 \ \ maxT$ **then**
    $impact \leftarrow 4$
  else if $assetValue \geq 0.4 \cdot maxT$ & $assetValue < 0.6 \ \ maxT$ **then**
    $impact \leftarrow 3$
  else if $assetValue \geq 0.2 \cdot maxT$ & $assetValue < 0.4 \ \ maxT$ **then**
    $impact \leftarrow 2$
  else
    $impact \leftarrow 1$
  return $impact/5$ ▷ `divide by 5 to interpret impact between 0 and 1`

Algorithm 2 Compute likelihood

procedure COMPUTELIKELIHOOD(t, rf) ▷ `Threat` t, `risk factor` rf
  $fe \leftarrow t.getFraudEnabler$
  $SL \leftarrow compareSkillLevel(rf.getSL_F, rf.getSL_D)$
  if $fe = eservice.ACTOR$ **then**
    $likelihood \leftarrow SL/3$
  else if $fe = eservice.ACTION$ **then**
    $u \leftarrow rf.getUnnoticeability$
    $likelihood \leftarrow (SL \times U)/6$
  else
    $SecL \leftarrow rf.getSecurityLevel$
    $likelihood \leftarrow (SecL \times SL)/9$
  return $likelihood$

Algorithm 3 Calculate risk

```
1: procedure CalcRisk(ts, rf, maxT)    ▷ List of Threats ts, risk factor rf
2:     for t in ts do
3:         impact ← computeImpact(t, maxT)
4:         likelihood ← computeLikelihood(t, rf)
5:         risk ← impact × likelihood
6:     return listOfRisks
```

Algorithm 4 Visualise risk

```
1: procedure GraphVisualizer(rs, rf)    ▷ List of Risks rs, risk factor rf
2:     set Y axis                                  ▷ values between 0 and 1
3:     for i= 0; i< rs.size(); i++ do    ▷ adding coordinates for all risks
4:         x_i.impact ← r.impact                                          ▷
5:         x_i.likelihood ← r.likelihood
6:         x_i.risk ← r.risk
7:         addbargraph(x_i)          ▷ addX − axisx_i three-level bar graph
8:     return listOfRisks
```

one or more risk factors depending on the nature of the threat scenario and considering the three cases described in the previous section.

Based on the results of the impact analyser and the pre-computed likelihoods, the risk is calculated as their product with a value in the interval $[0, 1]$. The output of this component is a list of threat scenarios with their associated risks. The graph visualizer presents these analysis results in different ways to support and enhance an informed decision making. It currently presents the calculated risks either as a single threat scenario or for the whole list of threat scenarios.

For a single threat, the graph visualizer presents the corresponding risk in a graph for all possible combinations of risk factors pre-calculated in the likelihood pre-computation. For instance, if the target of the threat is an actor action, the risk calculation is based on the skill level of the fraud agent, the skill level of the defender, and the action's noticeability. Based on the possible values, the risk values for relevant combinations are shown in a graph. Both presentations of risk values provide a range of tweaks to observe a high-level overview for potential risks on an e-service and more specifically the risk of a threat scenario to succeed.

Algorithms 1, 2, 3, and 4 show the pseudo-code for implementing the FRE architecture components described in Section 4.1, including impact analysis, likelihood computation, risk calculation, and graph visualisation.

4.2 Prototype Implementation

We have developed a stand-alone prototype[3] of FRE, shown in Figure 3. As mentioned in the previous sections, the inputs for FRE are a list of threat scenarios and an e-service model. The prototype takes only an e-service model as

[3] https://github.com/ahmedyesuf/FraudRiskEstimator/wiki

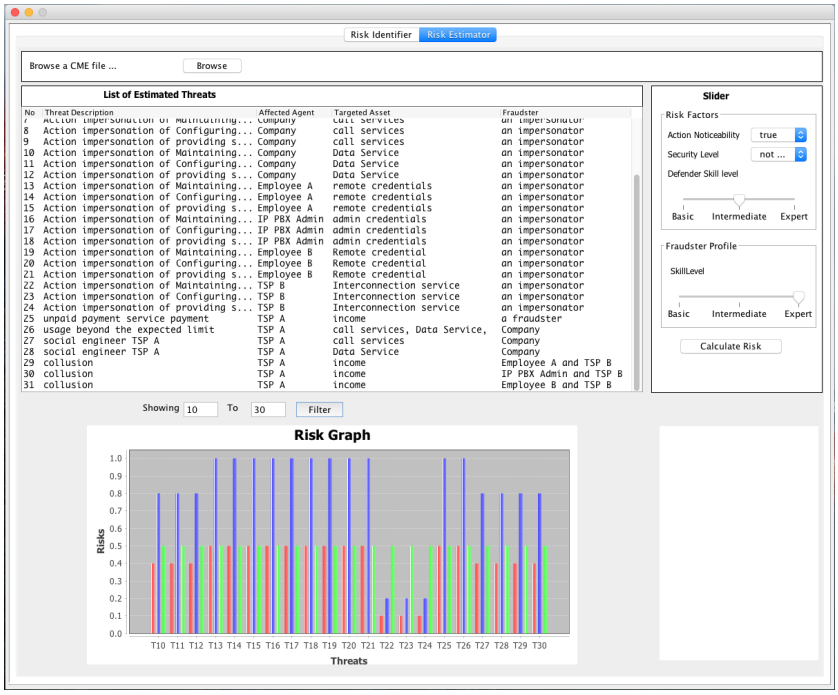

Fig. 3. Setting up risk factors in the FRE prototype.

input, and identifies threat scenarios from the model using pattern-based risk identification [14, 18]. Each identified threat contains the information described in Section 3 about the targeted asset, fraud enabler, affected actor, and potential fraudster.

Risk calculation is performed in two ways: for an individual threat scenario with all possible pre-calculated likelihoods, or for all threat scenarios with a given combination of risk factors, which we call *slider inputs*. These sliders allow an analyst to quickly change values of all variables, inspired by sliders in tools used in analysing MRI scans, where doctors do not look at the individual images, but quickly slide through the stack and look for discontinuities and rapid changes.

Based on chosen slider position, the calculated risks are visualised using graphs. The graph for individual threats as shown in Figure 4 helps to observe the risk factors that result in a threat scenario being above or below a certain risk level. The overview graph for all threat scenarios shown in Figure 5 helps to observe how many of the threat scenarios are found to be above or below a certain risk level given the specific combination of slider inputs. Both ways of presentation remarkably increase flexibility of displaying analysis results, and improve the process of an informed decision making.

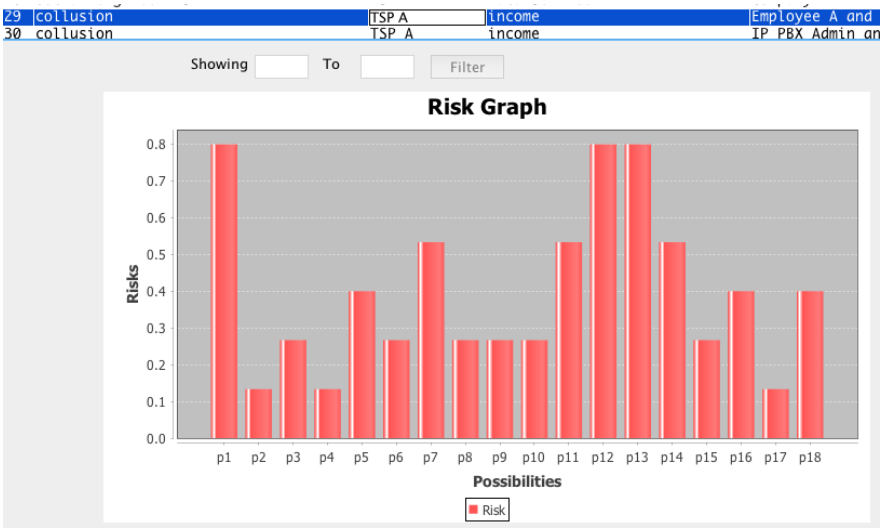

Fig. 4. Visualisation of possible risks for a single threat.

5 Case Study and Validation

We now apply the FRE framework to a case study from an e-service domain, namely a telecommunication service [17], and evaluate the performance of the FRE tool.

5.1 A Telecommunication Case Study

Consider a company that wants to use an IP-based Private Branch Exchange (IP-PBX) system in their communication system, and has created a post-paid contract with a Telecom service provider.

A postpaid contract is a type of service contract where users have to pay fees within a certain period of time, in this case every month, based on the usage of the IP-PBX service by the users of the company. Employees of the company are the main users of the IP-PBX system with an administrator to maintain and manage their services. Some of the IP-PBX services include call forwarding, call services (internal and external), and remote connections to the PBX system. An employee can use an IP-PBX service to communicate with internal or external parties, or to connect to the IP-PBX system remotely to get the same service if the feature is granted by the administrator. The service provider has the responsibility to transfer the calls and other types of services to the intended destination. For that, the service provider is supposed to create agreements with other service providers.

Threat scenarios. In this case study, different threat scenarios can be identified due to social, technical, and other weaknesses of the entities of the case study. To

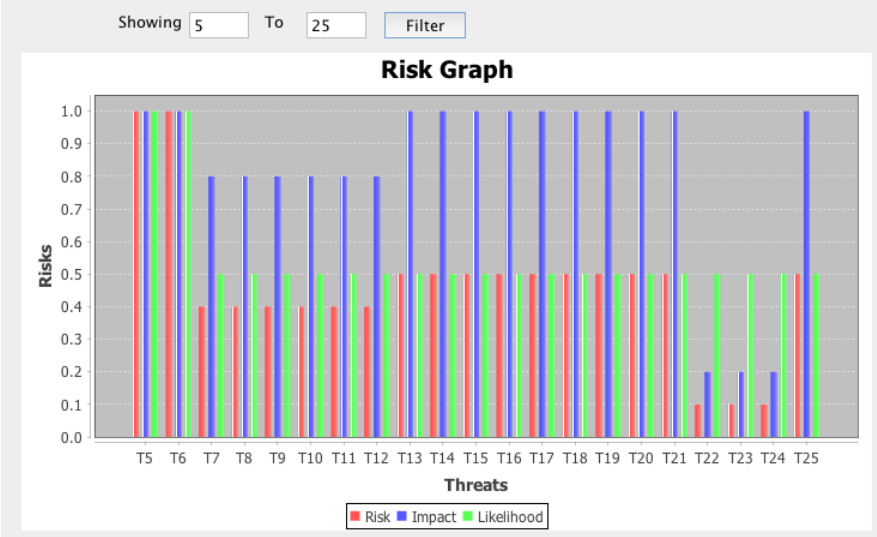

Fig. 5. Visualisation of possible risks for all threats.

identify them, we have used the *fraud threat model* designed by Yesuf [18] that provides us with recurrent problems occurring in most cases of e-service fraud. Fraud threats include impersonation of actors, time-interval misuses, usage of services beyond the expected limit, invisible collusion, insecure communication, and exploitation of infrastructure vulnerabilities. There are more than 31 possible threat scenarios identified in this cases study. The following are some of the threat scenarios from each threat model:

- Impersonation of employees to get remote credentials so a fraudster can use it to access the IP-PBX system; affected asset: remote credential; asset value: same value as direct assets with call and data service.
- Impersonation of IP-PBX admin to get admin credentials so a fraudster can use calling, administrating and maintain IP-PBX system; affected asset: admin credentials; asset value: the same or more than the asset value of calling, administrating and maintaining IP-PBX system;
- A fraudster pretends to deliver maintenance work to the Company so that the fraudster can get company call service and data service; affected asset: call service; asset value: the same or less than the contact fee between the service provider and the company;
- Unpaid service payment by the company for the services from the service provider; affected asset: service provider's contract fee; asset value: contract fee;
- Invisible collusion of employees of the company and the other service provider to increase the income of the other service provider which affects the main service provider's income; asset value: income of service provider; asset value: income of the main service provider.

Risk estimation. For the IP-PBX case study, the FRE framework computes and visualises impact, likelihood, and impact for the threat scenarios identified. We now discuss some of the threats.

The first case is the exploitation of remote credentials through an employee to establish calls. The remote credential is an indirect asset with a direct relation to the impact of call services. Thus, the impact of exploiting the remote credential is as big as the asset value of the call services. Assuming that call services account for 50% of the contract agreement, the impact of this threat is identified to be high.

Calculating the likelihood requires to identify the fraud enabler of the threat scenario, in this case an employee (actor). When the fraud enabler is an actor, the likelihood is calculated by comparing the skill level SL_f of the fraud agent and the skill level SL_d of the defender, which could be the company or the service provider. Since the skill level is difficult to assess, FRE pre-calculates the risk for all possible combinations of skill levels. The *likelihood pre-calculation* algorithm, for example, computes the likelihood to be intermediate if both SL_f and SL_d are *intermediate*. This results in risk of $0.8 \times 0.66 = 0.52$. As there are three possible values of skill level (basic, intermediate and expert), in total, FRE precomputes 9 different risk values that will be presented in a graph.

The second fraud we consider is enabled by *maintenance work*, which is an action. The risk factors for an action are its noticeability and as before skill levels of the fraud agent and defender, SL_f and SL_d, respectively. The action can be noticeable or not, so FRE pre-calculates 18 risk values.

For a fraud agent with intermediate skill level, an expert defender, and an unnoticeable action, the likelihood of the fraud agent to succeed is *unlikely*, due to a computed value of $(1 \times 2)/6 = 0.5$. Getting the company's call service access credential is worth the contract agreement, for which the impact is *very high (=1.0)*. The risk is therefore $0.5 \times 1 = 0.5$. This indicates that even though the impact is very high, the risk would be reduced by having good defense mechanisms. The risk can even be reduced further by increasing the noticeability of this kind of actions, for instance, requesting identity cards from the maintenance workers before allowing entrance.

The same calculations are performed for all threat scenarios. The resulting graphs for the IP-PBX case are shown in Figure 5.

5.2 Experiment: Performance Validation

The models generated for real world scenarios from different domains can be expected to become fairly large. To assess the scalability of the FRE framework when analysing large models, we now evaluate its computational performance.

The two FRE components that contribute to the computation are the risk calculator and the graph visualiser; the other components are inputs contributing to these components. The input for testing is a list of threats identified in the case study. To simulate the increased number of threats and observe the performance, we created larger models from the case study threats, and observed the response for several iterations. Figure 6 shows the test results, averaged over the iterations.

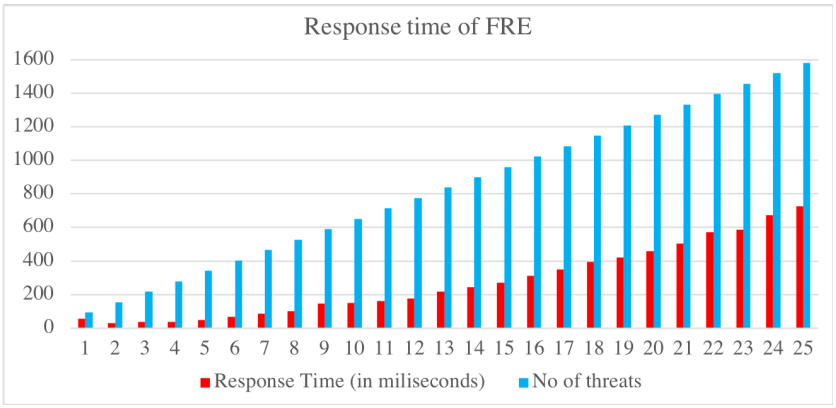

Fig. 6. The computational performance of FRE framework

The test result shows that the analysis time increases linear in the number of threats. The risk calculation takes insignificant time compared to the visualisation, since the computations in the former are relatively straightforward, while the visualisation uses an external graph library requiring more resources. Overall, for the objective of estimating risks for preventive measures, the prototype can accommodate the increased number of threat scenarios.

6 Discussion

Informed preventive measures on e-service fraud are strongly dependent on the analysis of possible threat scenarios on the target of the assessment and estimating their potential risks. The FRE approach enhances the risk analysis and estimation by providing an automated computation of risks from a given list of threat scenarios, visualisation the analysis results and supports repeated analysis when the context of the threat scenarios is changing.

The FRE approach leverages qualitative risk metrics to compute the impact and compute the likelihood of threat scenarios. This provides a number of advantages. It is impossible to compute absolute risk factors for new or revised version of an e-services, as there are limited input data about the risk factors beforehand. Pre-computing risks requires threshold values for risk factors of threat scenarios, and having these facilitates the analysis of risks based on possible combinations of risk factors. Thus, using qualitative risk metrics the FRE approach enables the automation of risk calculation and visualisation of analysis results.

Another strength of the FRE approach is its scalability. As the evaluation in the previous section shows, the response time increases linearly in the number of threats, meaning that also large models can be analysed in short time. This is an important factor for integrating FRE in a continuous risk assessment approach.

The FRE approach takes the e-service model as input, and uses it to obtain data of threshold values which uses to compute the impact of threat scenarios.

This does not mean that the risks computed by FRE are dependent on the e-service model, rather by providing the impact threshold as an input, it is possible to make the FRE approach independent from requiring e-service models as an input. The FRE approach currently targets e-services only due to the fact that our risk factors and metrics are produced from the perspective of the e-service domain. Yet the FRE approach can easily be extended to other domains by modifying and adding risk factors based upon the characteristics of relevant threat scenarios.

7 Conclusion and Future Work

E-services are characterised by rapid development, and continuous improvement and deployment. Designing and implementing a system or a service requires to perform risk analysis. Considering the characteristics of e-services, it is crucial to perform risk analysis and estimation automatically to support the decision-making process. In this regard, we propose the FRE approach to automatically compute risks from a list of threat scenarios, and to visualise the risks.

Fraud Risk Estimation remarkably reduces the time spent in computing risks using manual and traditional approaches by pre-computing the possible risk factors for threat scenarios. This allows risk analysts to perform iterative risk analysis by changing the context of threat scenarios within a very little amount of time.

Factors for which no estimates are available, or are considered to be untrustworthy, FRE introduces variables and computes the risk by making these variables assume all possible values. For these variables, we introduce sliders that allow an analyst to quickly change values of all variables. Sliders are inspired by those used in tools for analysing MRI scans, where doctors do not look at the indvidual images, but quickly slide through the stack and look for discontinuities and rapid changes.

In general, as cybercriminals are always coming up with numerous ways of committing fraud and attacks, security risk analysis needs to be supported with automated approaches to prevent security and fraud risks before it happens. Fraud Risk Estimation enables this approach. We are currently working with experts from different domains on applying FRE to case studies from their domain, in order to incorporate different risk factors for other types of threat scenarios.

References

1. Aagedal, J.O., Den Braber, F., Dimitrakos, T., Gran, B.A., Raptis, D., Stolen, K.: Model-based risk assessment to improve enterprise security. In: Enterprise Distributed Object Computing Conference, 2002. EDOC'02. Proceedings. Sixth International. pp. 51–62. IEEE (2002)
2. Abdallah, A., Maarof, M.A., Zainal, A.: Fraud detection system: A survey. Journal of Network and Computer Applications **68**, 90–113 (2016)

3. CFCA: Global telecom fraud report. Tech. rep., Communications Fraud Control Association (2015)
4. 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, pp. 289–306. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
5. Embley, D.W., Thalheim, B. (eds.): Handbook of Conceptual Modeling. Springer Berlin Heidelberg, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-15865-0
6. FAIR Institute: Fair (factor analysis of information risks) risk management (2018), https://www.fairinstitute.org/fair-risk-management
7. ISO/IEC Information security risk management: ISO 27005:2011, ISO 27005:2011 Information technology – Security techniques – Information security risk management (2011)
8. Johansen, I., Rausand, M.: Risk metrics: Interpretation and choice. In: Industrial Engineering and Engineering Management (IEEM), 2012 IEEE International Conference on. pp. 1914–1918. IEEE (2012)
9. McAfee CSIS: Net Losses: Estimating the Global Cost of Cybercrime. Tech. rep., McAfee and the Center for Strategic and International Studies (2018)
10. McEvoy, N., Whitcombe, A.: Structured risk analysis. In: Infrastructure Security, pp. 88–103. Springer (2002)
11. NIST: NIST cybersecurity framework, version 1.1. Tech. rep., National Institute of Standards and Technology (2018), https://www.nist.gov/
12. Probst, C.W., Willemson, J., Pieters, W.: The attack navigator. In: Mauw, S., Kordy, B., Jajodia, S. (eds.) Graphical Models for Security - Second International Workshop, GraMSec 2015, Verona, Italy, July 13, 2015, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9390, pp. 1–17. Springer (2016)
13. Riedl, C., Leimeister, J.M., Krcmar, H.: Why e-service development is different: a literature review. e-Service Journal **8**(1), 2–22 (2011)
14. Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., Sommerlad, P.: Security Patterns: Integrating security and systems engineering. John Wiley & Sons (2013)
15. Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M.: Taxonomy of information security risk assessment (isra). Computers & Security **57**, 14–30 (2016)
16. da Silva, A.R.: Model-driven engineering: A survey supported by the unified conceptual model. Computer Languages, Systems & Structures **43**, 139–155 (2015)
17. Yesuf, A.S.: MP-RA: Towards a Model-driven and Pattern-based Risk Analysis of e-service Fraud . In: Services 2018. Springer, Cham (June 2018)
18. Yesuf, A.S., Serna-Olvera, J., Rannenberg, K.: Using Fraud Patterns for Fraud Risk Assessment of E-services. In: 32nd International Conference on ICT Systems Security and Privacy Protection – IFIP SEC, pp. 553–567. Springer, Cham (may 2017)