A Review of Risk Identification Approaches in the Telecommunication Domain

Ahmed Seid Yesuf

Deutsche Telekom Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt, Frankfurt am Main, Germany
ahmed.yesuf@m-chair.de

Keywords: Risk Identification, Security, Telecommunication Service, Risk Assessment, Fraud Risk, Risk Management.

Abstract: Risks in the telecommunication (telco) domain are complex to identify due to the involvement of several independent stakeholders and the difficulty of predicting emerging threats to the services. This is costing the Telecom operators billions of dollars. We believe the little emphasis given to the important step of risk assessment process – risk identification (RI) – is the main reason for this loss. Unlike other domains, the proprietary nature of Telecom systems makes it challenging to show the risk assessment approaches in the domain. In this paper, we investigate the classifications of the RI approaches from the literature written on the telco and other related domains. We also investigate the research trends in the last 16 years when Telecom risks are evolving and the revenue loss of Telecom operators is largely affected. Based on our review, we also show future research directions in the domain.

1 INTRODUCTION

The lives of people are changing through time since the beginning of telecommunication (telco) services. Individuals able to communicate with their families, friends and relatives from almost anywhere using data, voice or video communication services. Companies and organisations facilitate their tasks better than ever using the telco services. Telecom companies strive to deliver their services considering customers’ information security and privacy requirements into consideration. It is also obvious that they want to protect their revenue stable and profitable. The responsibilities of a Telecom companies include accepting, delivering and transmitting the message from a sender to a recipient. Typical telco services are roaming, VoIP, PBX service, national and international messaging and call services. Unfortunately, attackers or fraudsters are working to deform the telco services to gain individual or organised benefit, for instance, using the service without payment.

According to the Communication Fraud Control Association (CFCA)/(CFCA, 2015), fraud is the use of telco services or products with no intention of payment. Thus, fraud negatively affect the global telco revenue. In 2015, fraud affect the global Telecom revenue by almost $38.1 billion USD. It is lower from the previous reporting years because the Telecom operators outsource their fraud risk management to the third party companies. Even though there is momentum in reduction of fraud loss from 2009, it requires a lot of work in risk reduction from the Telecom operators’ perspective. The estimated global loss from 2000 is shown in Table 1. The two top most sustainable fraud categories from the year 2000 are subscription and PBX hacking, where the loss in 2013, for instance, is $5.22 and $4.42 billion USD respectively.

Despite the fact that the Telecom industry loses billions of dollars every year due to several types of risks (socio-technical-economic risks), the control measures are not handling to stop risks from happening. The reasons are due to the following problems: 1) risks in the Telecom industry are not straight forward to identify how they could happen, 2) the existing risk assessment process in the Telecom industry couldn’t cope up with those complex, dynamic and sophisticated attacks/fraud, and 3) researches on risk assessment techniques are limited in the telco domain to handle those risks. In this paper, we are interested in business related and socio-technical risks, but we use the general term risk to indicate also other types of risks - fraud risks, performance and security risks.

In order to address problems, the risk assessment process – specifically the risk identification (RI) stage - plays an important role. There are different types of RI approaches in the research community specific to the field of studies. In this paper, we perform a systematic review to find out the existing RI approach-
Table 1: Yearly fraud loss (in billion USD) based on CFCA (CFCA, 2015).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss</td>
<td>$35.0</td>
<td>$46.3</td>
<td>$38.1</td>
<td>$40.1</td>
<td>$46.3</td>
<td>$72.8</td>
</tr>
</tbody>
</table>

...ex/techniques available in the domain. This helps us to identify the research landscape and shape future research directions. Section 2 describes the scope and methodology used for the review; Section 3 discusses the findings including the research trends in the last 16 years. Finally, Section 4 highlights open issues and future research directions of risks identification in the domain.

2 SCOPE AND METHODOLOGY

Scope. To shape the scope of the review process, we use Coopers literature review taxonomy (von Brocke et al., 2009). The focus of the review is to investigate and analyse the research outcomes and applications of the RI approaches. This happens by exhaustively searching publications in the telco domain and related domains. The goals of the review are: 1) identifying and classifying the RI approaches with their applicability to the telco domain: the review mainly focuses on the RI methods, frameworks or approaches of the telco domain. But we also investigate the RI approaches from related domains, e.g. e-commerce, communication systems and network systems, in order to find out approaches that are applicable to the telco domain. 2) Finding out the research trends in the domain: in order to understand the trends of the literature, we exhaustively search the selective keywords in each database for publications from 2000 to 2016. This is because since 2000 risks in the domain get sophisticated and costs the Telecom operators billions of dollars (CFCA, 2015).

The general audience of the review include experts, scholars or practitioners in the telco sector. Therefore, the selection of databases and keywords is based on the above taxonomy.

Methodology: Search Resources. In order to span several databases of literature in the selected domains, we use well-known publishers in several disciplines: IEEE, Springer, and ACM from the area of Computer Science; AiSeL from the areas of Information Systems; Elsevier from several disciplines spanning from Computer Science, Engineering, E-commerce, and Telecommunication. The combined search results from these databases provide the big picture of the domain. The keywords are carefully selected to span the problem domain. Besides, we include keywords related to e-commerce and communication systems in order to observe how the problem is addressed in the related field of studies. Even though the searching mechanism varies from one database to another, we kept the main scheme of our keywords in all of the selected databases. The main query keywords are shown below.

```{("risk identification" or "risk analysis" or "risk analyses" or "risk assessment" or "risk management")
and (method or approach or framework)
and (e?commerce or "communication system" or "telecommunication")
not {agriculture or oil or volcanic})```

3 FINDINGS

By searching the keywords in the databases above, 44 representative papers are filtered after fifth iterations. The summary of iterations is listed in Table 2.

3.1 Classes of RI Approaches

RI is the process of finding out several types of risks in an enterprise before, and after the system is developed or the service is released to the customers. The RI approaches of the telco domain are limited in number from the literature identified above but the fact that we extended the search to the related domains (e.g. e-commerce, communication networks and systems) provide several other types of approaches which can be extended and applicable to the telco domain. From this, nine different RI classes of approaches are identified which allow us to classify the 44 papers observed above. As the classes are produced considering the perspective and emphasis of each paper (the input for RI, the model leveraged, the security standard they use), it can be extended to be used to observe papers in similar domains. The following classes are produced. The classification of RI approaches with respect to the selected literature is shown in Table 3.

Model-based security engineering (MBSE): is a strategy of assessing risks against the security requirements/policies based on different types of system models (e.g. system architecture, use-cases, sequence, deployment diagrams). These models provide the possibility to understand the context of the risky environment, which in the end need to be analysed. Some of the MBSE approaches identified in the literature include CORAS/Aagedal et al., 2002; Gran...
Table 2: Number of publications in each database.

<table>
<thead>
<tr>
<th>Databases</th>
<th>IEEE</th>
<th>ACM</th>
<th>Springer</th>
<th>Elsevier</th>
<th>AiSeL</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st iteration (first search)</td>
<td>657</td>
<td>749</td>
<td>694</td>
<td>582</td>
<td>284</td>
<td>2966</td>
</tr>
<tr>
<td>2nd iteration (filtered by the titles)</td>
<td>128</td>
<td>40</td>
<td>61</td>
<td>40</td>
<td>22</td>
<td>291</td>
</tr>
<tr>
<td>3rd iteration (filter by the abstracts)</td>
<td>55</td>
<td>20</td>
<td>8</td>
<td>11</td>
<td>11</td>
<td>105</td>
</tr>
<tr>
<td>4th iteration (filter by the contents)</td>
<td></td>
<td></td>
<td>42</td>
<td></td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>5th iteration (with backward search)</td>
<td></td>
<td></td>
<td></td>
<td>44</td>
<td>44</td>
<td></td>
</tr>
<tr>
<td>Total number of publications observed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>44</td>
<td></td>
</tr>
</tbody>
</table>

Discussion: The Result. Model-based risk assessment approach is proposed for telco domain in (Jurjens et al., 2008) and (Vinnakota, 2011). UMLsec - one of model-based approaches and the extension of UML modelling - is used to identify and analyse risks in mobile communication systems (Jurjens et al., 2008). It provides the possibility of integrating security requirements (basically security policies) of a Telecom enterprise into the development of a secured system. In (Vinnakota, 2011), Cybernetics Risk Influence Diagraming (CRID) is used to identify interconnected, interrelated and emerging risks in a software project, which is applicable to the Telecom domain. CRID begins its process by identifying risk influencers - events or conditions - that lead for a risk to happen. With the involvement of project manager and team members of a project, the influence of each risk influencers will be identified. This process iterates at each stage of the project life cycle to identify and evaluate risks of the project. Some papers from the related domains have proposed security risk modelling and assessment approaches of their IT systems and services (Mounzer et al., 2010), (Dantu et al., 2004), (Aagedal et al., 2002), (Sadiq et al., 2010), (Zalewski et al., 2013), (Nostro et al., 2014), (Cholez and Feltus, 2014), by which some of them are applicable in the telco domain. To mention some of the others, the RI process in (Mounzer et al., 2010) is a structural way of identifying threats and the corresponding attacks against the crucial assets of a system, even though the main focus is given to the assessment and mitigation stages of the risk management process. Based up

---

1 STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (msdn.microsoft.com).
<table>
<thead>
<tr>
<th>Classes of RI approaches</th>
<th>Known approaches from the selected literature</th>
<th>Literature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat modelling</td>
<td>STRIDE, DREAD, fault tree</td>
<td>(Prasad, 2007) (Zalewski et al., 2013)</td>
</tr>
<tr>
<td>Business process based RI</td>
<td>Mapping business process with the probabilities of failure, impact analysis</td>
<td>(Ernawati et al., 2012) (Mayer and Aubert, 2014) (O’Donnell, 2005) (Rohde et al., 2016)</td>
</tr>
<tr>
<td>Data mining</td>
<td>Fraud detection algorithms</td>
<td>(Harantzis and Malek, 2004) (Bihina Bella et al., 2009) (Brucker et al., 2010) (Subudhi and Panigrahi, 2015) (Tseng et al., 2015)</td>
</tr>
<tr>
<td>Game Theory</td>
<td>Attacker-defender model</td>
<td>(He et al., 2008)</td>
</tr>
<tr>
<td>Survey and Brainstorming</td>
<td>Questions-Answers, discussions, SWOT analysis, SJT, existing literatures</td>
<td>(Mounzer et al., 2010) (Sadiq et al., 2010) (Rippon, 2006) (Martinez-moyano et al., 2006) (Esteves et al., 2004) (Herzfeldt et al., 2012) (Macwan, 2004) (Sutton et al., 2008) (Rohde et al., 2016)</td>
</tr>
<tr>
<td>Probabilistic analysis</td>
<td>Bayesian networks; Failure of system, router</td>
<td>(Dantu et al., 2004) (Vidalenc and Cavaglia, 2010) (Sherif et al., 2003) (Wickboldt et al., 2011) (Cortellessa et al., 2005)</td>
</tr>
</tbody>
</table>

Table 3: Classification of RI approaches.

on the preliminary RI process, the risk modelling and control/mitigation is performed through graph-based approach and mathematical optimisation respectively. In order to estimate risks of a critical resources in an enterprise, (Dantu et al., 2004) argues that identifying the behaviour of attackers play an important role. A behaviour-based attack graph is used to show their argumentation. Another model-based enterprise risk assessment approach called CORAS (Aagedal et al., 2002; Gran et al., 2007) uses modelling of unwanted incidents, vulnerabilities and threat scenarios of a system to identify risks against the target of assessment.

Threat modelling is also used as an approach to identify risks. It is the process of identifying threats structurally using standard threat models, e.g. STRIDE, DREAD (Prasad, 2007) or fault trees (Prasad, 2007); in this regard, besides integrating other model-based risk assessment models, (Zalewski et al., 2013) and (Prasad, 2007) leveraged Microsoft STRIDE threat model and fault trees to analyze the security of cyber-physical systems and enterprise risks respectively. Even though some of the literature above follows structural analysis together with the model-based approach, there exist literature which only used the structural analysis - identify assets, vulnerabilities, threats to find out security risks (La Corte and Scatà, 2010) (Rossebø et al., 2007) (Yu and Wu, 2010) (Iannicca et al., 2013) (Rippon, 2006) (Tsai and Huang, 2011). The approaches from (La Corte and Scatà, 2010), (Rossebø et al., 2007), (Yu and Wu, 2010), and (Rippon, 2006) are applied in the telco domain.

Some of the RI approaches use business processes to identify risks in an enterprise (Ernawati et al., 2012), (Mayer and Aubert, 2014) and (O’Donnell, 2005), where the first two papers applied the approach for the telco domain. Some others, (Harantzis and Malek, 2004) (Bihina Bella et al., 2009) and (Brucker et al., 2010) describe and use approaches of data mining for identifying fraud risk in the telco domain.

Under the class of Standards and Methods, security standards and other known methods (e.g. Ha-Zop) are used in the risk assessment and management process including RI (Mounzer et al., 2010) (Aagedal et al., 2002) (Ernawati et al., 2012) (Mayer and Aubert, 2014) (Stoneburner et al., 2002) (Vahl et al., 2009) (Seify and Bijani, 2009) (Bojanc and Jerman-Blažič, 2008).

Discussions, SWOT analysis, existing literature and survey are also considered as a way to identify different types of risks in (Mounzer et al., 2010) (Sadiq et al., 2010) (Rippon, 2006) (Martinez-
moyano et al., 2006) (Esteves et al., 2004) (Herzfeldt et al., 2012) (Macwan, 2004) (Sutton et al., 2008).

Research Focus of the Selected Papers. We show the results using the RFC 2904 requirements (Vollbrecht et al., 2000) that helps to categorise the focus of the selected papers based on the authorisation level: single domain case (SDC) and distributed domain case (DDC). In a single domain case (SDC) there exists only one administration domain that put decisions on different aspects; everything else is grouped into a distributed domain case (DDC). Considering the context of the telco as a system or a service released to customers, we further have three subcategories of applicability: before, at real-time and after a system is developed or a service is released to customers. The distribution of the selected papers in the telco and other related domains is shown in Figure 1. Open research gaps in SDC domain include threat modelling approaches, game theory and data mining. In addition to these, structural analysis, business process based RI, and probabilistic analysis are the research gaps in the domain of DDC. This helps to understand the research landscape of the telco domain and other domains (specifically e-commerce and communication systems).

In general, we draw the following key points: 1) Risks in the telco domain are continuous and happen in variety of forms, but the RI approaches only apply to specific domains. 2) The review based on public researches on this area only reveals the partial image of the problem. The challenges include lack of enough publication resources, difficulty of getting real telco data to do researches and willingness of the Telecom operators for external researchers.

3.2 The Research Trend

In the first five years, mobile applications, the development of application software for smart phones and the next generation networks (NGN) were the topic of discussion. The risk management and assessment approaches were, therefore, targeting such trend to identify risks, analyse the impacts and provide counter-measures of different types of risks (including human factors).

From the beginning of 2006, IP-based telco services, as the main part of NGN, were widely adopted to provide the complementary functionalities to the classic audio, messaging and data services. Since then the research trend were extended to risk assessment of the NGN networks and associated elements that go together with it, including risks of network infrastructures, mobile applications development, fraud risks and leakage of customers information. Several risk assessment and management approaches were proposed. More than 30% of the selected telco papers lied between 2006 and 2010.

In continuation to the above trend, due to the introduction of NGN, the Telecom enterprise have enforced to work together with other enterprises including banks. This relationship also produced new business and security risks. The regulatory bodies modify the existing regulations on the telco services based on the new types of services. So flexible ways of risk management and assessment approaches were the main focus of discussions. Table 4 summarises the main focus of the selected papers and the types of telco risks with in different years of time.

4 CONCLUSION AND FUTURE RESEARCH DIRECTIONS

The RI approaches identified above cover some of the telco risks in the domain. We believe telco risks can be minimised through investigation of specific problems and researching suitable approaches, which can prevent risks before occurring or before the damage escalates beyond a threshold. From this perspective the following are future research directions on identification of telco risks.

Usage of model-based security engineering (MBSE) for several types of risks: MBSE is applicable to many of risk assessment problems in the telco domain. From the review, (Jurjens et al., 2008) shows how the security policies of a company can be enforced and verified on telco network architectures and communications. This is the effort of involving MBSE.
Table 4: The research trends between 2000 and 2016, based on the selected papers.

<table>
<thead>
<tr>
<th>Years</th>
<th>Types of risks</th>
<th>Main focus</th>
<th>Literature</th>
</tr>
</thead>
</table>

in the development of mobile applications. An interesting development could go beyond enforcement of security requirements. For instance, **MBSE** can itself help in identifying other security, transaction, and privacy risks. The combination of **MBSE** models can also represent other risks as shown from some of the papers from related fields (e.g. (Dantu et al., 2004) shows how behaviour based attack graph can be used in assessing enterprise risks). In this regard, the EU project TRESPASS (Montoya, 2013; Pieters et al., 2014) strives to come up with a modelling approach which identifies, analyse and prioritize socio-technical risks covering the telco domain.

Unlike for other domains, **real-time RI approaches** of the telco domain identify risks after the damage has occurred. In a call service, for instance, a real-time RI approach detects only after some amount of call traffic has been inflated. Unfortunately, the damage has already been done even though the risk has been detected. Therefore, a RI and assessment approach that takes the call payment plan, telco services architecture and surrounding context into consideration is an interesting research direction which prevent risks before happening.

Risks in distributed domain case, for instance roaming, involve multiple operators where the authorisation level for each of operators is different. Risks emerge not only from the weaknesses of the home operators but also due to existing settings of other operators. A new requirement of a RI approach from this regard is that it should engage the existing settings of the surrounding environment. From our review, we identified data mining approaches and business process based approaches are open issues that could address such problems when they are designed to a specific set of problems involving several authorization levels. Other types of RI approaches including game theory, threat modelling and probabilistic analysis are also the potential approaches that can be applicable together with other types of approaches.

Data mining approaches are observed strong in RI and real-time risk detection. Through identifying patterns of the risky situation, this approach detects risks at real-time. The fact that risks are detected after the damage has been done limits the full functionality of this approach. Instead, preventive RI approaches (e.g. analysis of service contracts and policies) can help develop the maximum possible prevention and detection capabilities.

As new technologies get increased, the risk assessment approach should also adopt the changes to prevent emerging risks. Fraud risks could emerge due to the tariff plan of operators, social engineering attacks, flawed business processes and transaction failures. A RI approach, therefore, should consider internal and external risk motivating factors (e.g. the security level of employees and market competition respectively).

In general, due to the complication of risks in the telco domain, the risk assessment steps should also be designed taking such complication into considera-
tion. In this regard, this paper provides an overview of classes of RI approaches, investigate the research trends and future research directions of risk assessment steps in the telco domain.

ACKNOWLEDGEMENTS

Part of the research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TREsPASS). This publication reflects only the authors’ views and the Union is not liable for any use that may be made of the information contained herein.

REFERENCES


Mayer, N. and Aubert, J. (2014). Sector-Specific Tool for Information Security Risk Management in the Con-
text of Telecommunications Regulation (Tool demo).

In Proceedings of the 7th International Conference on
Security of Information and Networks - SIN ’14, pages

Montoya, L. (2013). The trespass project.

Mounzer, J., Alpcan, T., and Bambos, N. (2010). Inte-
grated security risk management for IT-intensive
organizations. In 2010 6th International Conference on
Information Assurance and Security, IAS 2010, pages
329–334. IEEE.

Nostro, N., Ceccharelli, A., Bondavalli, A., and Brancati, F.
(2014). Insider Threat Assessment. ACM SIGOPS

systems-thinking framework for the event identifica-
tion phase. International Journal of Accounting

Pieters, W., Hadziosmanovic, D., Lenin, A., Monto-
analysis (poster).

Prasad, N. R. (2007). Threat model framework and method-
ology for Personal Networks (PNs). In Proceedings of
the 2007 2nd International Conference on Commu-
nication System Software and Middleware and Work-
shops, COMSWARE 2007, pages 1–6. IEEE.

systems. In 1st IEEE Workshop on VoIP Management

Routines in the Face of Fraud. AMCIS 2016 Proceed-
ings.

ETVRA, a threat, vulnerability and risk assessment
method and tool for eEurope. In Proceedings - Sec-
ond International Conference on Availability, Reli-

Sadiq, M., Rahmani, M., Ahmad, M., and Jung, S. J. S.
(2010). Software risk assessment and evaluation pro-
cess (SRAEP) using model based approach. In Net-
working and Information Technology (ICNIT), 2010
International Conference on, pages 171–177. IEEE.

Network Security Risk Management. In 2009 Sixth
International Conference on Information Technology:
New Generations, pages 1572–1573. IEEE.

management for new service introduction in telecom-

SP 800-30. Risk Management Guide for Information
Technology Systems.

Subudhi, S. and Panigrahi, S. (2015). Quarter-Sphere Sup-
port Vector Machine for Fraud Detection in Mobile
Telecommunication Networks. Procedia Computer

Sutton, S. G., Hampton, C., Khazanchi, D., and Anrold, V.
(2008). Risk Analysis in Extended Enterprise Envi-
ronments: Identification of Critical Risk Factors in

Tsai, H.-Y. and Huang, Y.-L. (2011). An Analytic Hi-
erarchy Process-Based Risk Assessment Method for
Wireless Networks. IEEE Transactions on Reliabil-
ity, 60(4):801–816.

Tseng, V. S., Ying, J.-C., Huang, C.-W., Kao, Y., and Chen,
ACM SIGKDD International Conference on Knowl-
edge Discovery and Data Mining - KDD ’15, pages

Vahl, M., Boehmer, S., and Oestreich, T. (2009). Probabil-
ity Based Risk Analysis for a VoIP System. In 2009
Fifth Advanced International Conference on Telecom-
munications, pages 441–446. IEEE.

Vidalenc, B. and Ciavaglia, L. (2010). Proactive fault man-
agement based on risk-adjusted routing. In IEEE
Globecom Workshops, GC ’10, pages 481–485. IEEE.

projects: A systems and Cybernetics approach. In
2011 IEEE International Conference on Quality and
Reliability, ICQR 2011, pages 376–380. IEEE.

Vollbrecht, J. R., Calhoun, P. R., Farrell, S., Gommans, L.,
Gross, G. M., Bruijn, B. D., Laat, C. T. D., Holdrege,
Framework Status. pages 1–35.

von Brocke, J., Simons, A., Niehaves, B., Riemer, K., Platt-
flaut, R., Cleven, A., Brocke, J. V., and Reimer, K.
(2009). Reconstructing the Giant: On the Importance
of Rigour in Documenting the Literature Search Pro-
cess.

Wickboldt, J. A., Bianchin, L. A., Lunardi, R. C., Granville,
framework for risk assessment based on analysis of
historical information of workflow execution in IT

enterprise vulnerability management. In Proceedings of
the 2011 conference on Information technology ed-
cation - SIGITE ’11, page 257, New York, New York,
USA. ACM Press.

formation in telecommunication industry. In Proceed-
ings - 2010 International Conference of Information
Science and Management Engineering, ISME 2010,
volume 2, pages 341–344. IEEE.

Zalewski, J., Drager, S., McKeever, W., and Kornecki, A. J.
(2013). Threat modeling for security assessment in
cyberphysical systems. In Proceedings of the Eighth
Annual Cyber Security and Information Intelligence
Research Workshop on - CSRFIRW ’13, page 1, New
York, New York, USA. ACM Press.

396