Analysis and Modelling of Fraud and Revenue Assurance Threats in Future Telecommunications Network and Service Environments

Jogesh Patel

France Telecom R&D UK Ltd. and University College London

Abstract: Fraud Management and Revenue Assurance (RA) are both key factors in maintaining operators margins, and with the growth in complexity of networks and services and with the increasingly sophisticated use of technology by fraudsters, these functions require an end-to-end approach which proactively identifies future challenges. This paper aims at proposing two approaches to provide ways of identifying Fraud and RA threats that arise as a result of the anticipated technological changes and categorising the risk associated with each identified threat in order to propose a set of mitigating measures that can allow for practical fraud management and revenue assurance in future telecommunication network and service environments.

1. Introduction

In criminal law, fraud is the crime or offence of deliberately deceiving another in order to damage them, usually, to obtain property or services from him or her unjustly [1]. The Telecommunications (Fraud) Act 1997 [2] was an Act to amend the Telecommunication Act 1984 to make further provision for the prevention of fraud in connection with the use of a telecommunications system. From a telecom operator's viewpoint, Fraud is recognised where a process, control or a technical weakness is exploited (usually via deception) to obtain an advantage. Typically the fraudsters secure a financial benefit for themselves by gaining access to services and content with paying for it and then reselling access to it to others. Subscription fraud and Identity (ID) Theft are the most common types of telecom fraud.

Revenue Assurance is the process that a telecom operator uses to ensure that all revenues due for the services provided to customers and 3rd parties are accurately billed, accounted for and completely collected whilst managing fraud to an acceptable level. It is commonly accepted amongst Fraud and RA consultancies that the level of financial loss incurred by telecommunications operators in relation to Fraud and RA typically ranges between 1% and 5% of revenues. The GSM Association estimates that annual fraud losses globally are in excess of $40 billion and rising [3].

Communications consumer behaviour has undergone a rapid evolution during the last decade. This evolution has mainly been driven by the need to offer customised and personalised services and applications seamlessly to users in a ubiquitous manner. Major changes will take place in existing telecommunications network and service infrastructure to offer new and converged services across heterogeneous access networks and to a wide range of end user devices. This transformation will bring with it new challenges to operators in regard to securing their new and evolving infrastructure from fraud and revenue assurance threats.

An essential part of this technological evolution will be the replacement of traditional circuit switched networks (PSTNs) with more flexible and open packet switched systems built on standardised Internet protocols and network architectures such as SIP [4] and IMS [5]. The move to an All-IP core network creates a merging of the mobile and internet worlds and meets the demand for converged services involving voice, video and data, while maintaining access to legacy systems. Whilst modern standards and products for providing VoIP/IMS calls and services are highly developed, concepts and technologies for securing VoIP infrastructure are still in early maturity. Security threats such as VoIP session hijacking, VoIP eavesdropping and Denial of Service attacks from the internet realm will now have to be detected, managed and prevented in the converged (mobile, fixed & ISP) realm.

2. Bottom-Up vs. Top-Down

In order to analyse and model Fraud and RA threats in future telecommunications network and service environments, two approaches are identified. The traditional bottom-up approach assumes prior knowledge of existing and known security, fraud and RA threats and applies these to the new network

architecture or service design. The first opportunity at which the bottom-up approach is addressed is from both a technical and non-technical Fraud and RA perspective to ensure that appropriate protection measures are integrated into the network and service design stages. The design of a service usually involves decisions around pricing models; these can be assessed by RA analysts to identify if previous causes of known revenue leakage have been 'designed out' of these new services. The second opportunity at which it is addressed is at the testing and evaluation phases of the network or service prior to deployment within an end-to-end system environment. The third and last opportunity concerns the deployment of a range of detective fraud controls; these may include sophisticated Fraud Management Systems (FMS) but will also comprise many other process based controls deployed transversally across the enterprise. A FMS is used to primarily address fraud issues, there is equally a range of controls that are deployed to detect revenue leakage; these can again be system based (e.g. Test Call Generation systems, Data Reconciliation systems) or process based (e.g. Change Management process). The objective of the bottom-up approach is to ensure that new technical environments and services are designed and implemented to mitigate the risk against known Fraud and RA threats within existing mobile, fixed and ISP operators, by reducing the probability that these threats will materialise and/or by increasing the likelihood of early detection of any risks that do materialise.

The research being conducted as part of this paper aims to model a top-down approach for the identification of first Fraud and RA threats. These are previously unknown Fraud and RA threats that arise from the design, development and deployment of new networks and services. In the top-down approach a view of the enterprise is formulated and used to build abstractions that help to understand, communicate and capture business processes and identification of functional requirements, non-functional requirements and external constraints related to the specified system/service. Use case modelling is applied at this stage to understand the behaviour of threat agents in the operational environment. A threat agent is a person or a thing, which acts, or has the power to act, to cause, carry, transmit or support a threat. The enterprise view is then refined further to perform system modelling which concerns the target logical system architecture, service design and information objects. This stage of the modelling process provides a view on how the logical components and tiers of the system are tied together and how they inter-operate. The analysis of Fraud and RA threats to target network architectures such as IMS can be performed by using Fraud and RA threats identified through the bottom-up approach and applying these to the system architecture, service and information models in order to validate their applicability. More importantly the system modelling activity may provide through the process of gap analysis, the opportunity to identify security vulnerabilities within the target system or service that result in the identification of new Fraud and RA threat opportunities for the fraudster. The system view is then finally refined to perform implementation modelling which results in the identification of new requirements, functions and practical mechanisms through which existing or new Fraud and RA threats may be detected, measured and prevented by telecom operators. The implementation modelling activity concerns the mapping to infrastructure, implementation of component specifications, system integration and testing.

3. International Revenue Share Fraud

One example of existing and known fraud identified through the bottom-up approach is International Revenue Share Fraud (IRSF) and involves organised groups using fraudulently obtained connections to make a high number of calls into high cost 'revenue share' service numbers while roaming. IRSF is costing the telecom industry millions every year. Figure 1 shows the stakeholders that are concerned during an IRSF scenario and describes the following sequence of events:

1. Fraudster uses techniques such as identity theft in order to impersonate a legitimate customer.
2. Fraudster uses this stolen identity to fraudulently obtain subscriptions in the originating country.
3. Fraudster delivers SIM cards to a second country where roaming is activated.
4. Fraudster uses these subscriptions to call premium rate numbers in a third country.
5. Customer is charged by Home PLMN for premium rate calls made by the Fraudster.
6. Home PLMN pays for the roaming charges to Visited PLMN.

7. Visited PLMN pays fixed line interconnects costs to Fixed Line Operator.
8. Premium rate revenues are generated at the Revenue Share Service Provider.
9. Revenues are then collected by the fraudster and the networks are left with unpaid invoices and settlement of roaming charges.

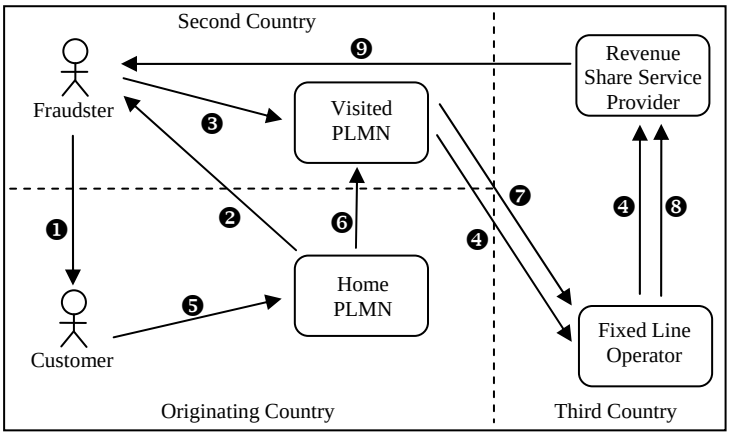

Figure 1: International Revenue Share Fraud scenario

4. Converged Telecommunications Network and Service Environment

One approach of applying top-down modelling is to begin with an abstract generalisation of the target evaluation environment as shown in Figure 2. The *user* is a person or entity that has subscribed to access and use services that are offered by the communication system. The *victim* is an individual or an organisation that has been subjected to fraud and as such has incurred loss of service or financial assets. The *threat agent* is an individual, group or a thing that can manifest a threat to the communications system in order to generate a personal or financial gain. It is important to note, that the *victim* and the *threat agent* can both be a *user* of the communication system. The *interconnect/roaming partner* is an organisation or communications infrastructure provider that allows for the extension of connectivity service to the communication system to a location that is different from the home location where the service was registered. The *3rd party* is a person or an organisation that provides a service to and via the communication system such as a content provider. The *stakeholder* is a person or entity that represents either a corporate, regulatory, legal, financial, auditory, enforcement, security or technical responsibility for the communications system. Lastly, the *communication system* is the target of evaluation and represents the telecommunications network and service infrastructure within the converged communications environment.

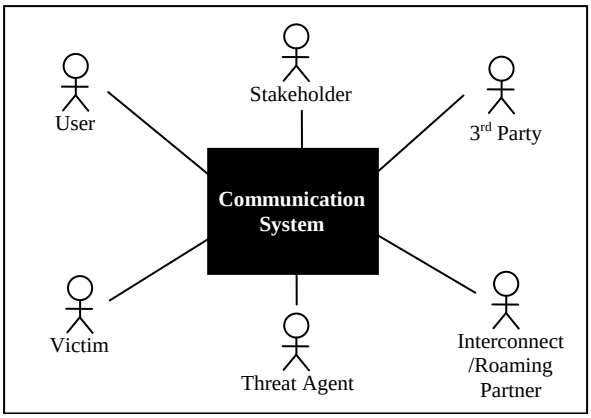

Figure 2: Fraud in a converged communications environment

The communications system represented in Figure 2 is further refined to reveal the systems that are present within the converged telecommunications network and service environment. A functional representation of the communications system is shown in Figure 3 and aims to identify points in the system architecture which can be modelled for security vulnerabilities, Fraud and RA threats. The emergence of sophisticated user equipment running on open operating systems that support multiple protocols offers the fraudster the opportunity to exploit security vulnerabilities through malicious software to create Fraud. Threat agents can exploit known vulnerabilities to gain unauthorised and therefore free admission to the access network to use the network and services in a fraudulent manner to generate revenue for the fraudster. Core network elements and systems such as IMS can be modelled for Fraud and RA threats. The need for operators to open up their network capabilities

through the service plane using APIs may pose threats committed by and via 3rd party service providers. Relationship with interconnect and roaming partners require to be modelled in order that operators can act without delay to mitigate the exposure to fraudulent traffics between their networks. The move to an All-IP core network increases the ways in which both traditional services can be accessed and new services can be implemented. The operator needs to understand how security, Fraud and RA threats will map and apply from the internet to the converged telecommunications network and service environment of the future.

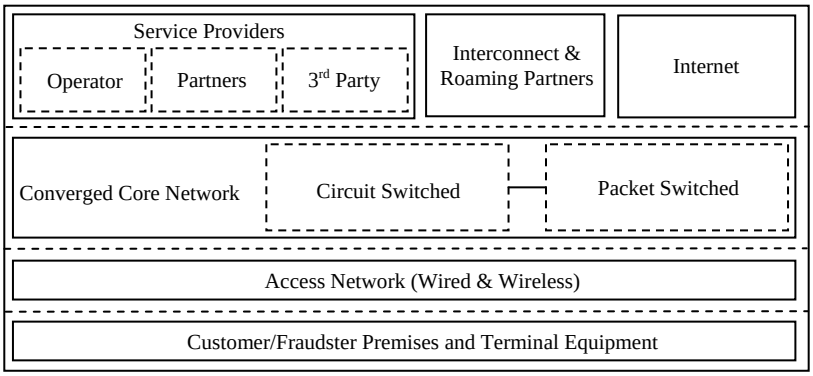

Figure 3: Converged telecommunications network and service environment

5. Conclusions and Future Work

This paper has provided an overview of Fraud and Revenue Assurance and through examples shown how two approaches can be used to model existing, and identify new Fraud and RA threats within future telecommunications network and service environments. The work presented in this paper serves as a first step to the design of a Fraud and RA threat model and the following areas of exploration are considered for future research:

- Investigate the use of modelling techniques and such as Object Orientation and UML [6] to capture the behaviour of different Fraud and RA threats in the operational environment.
- Assess the suitability of the ISO Reference Model for Open Distributed Processing (RM-ODP) [7] to define architecture and design a methodology for the modelling of Fraud and RA threats in a converged environment.
- Perform analysis and comparison of the pros and cons of the top-down vs. bottom-up approaches for Fraud and RA threat modelling.

Acknowledgements

The author would like to acknowledge advice and support from Dr Miguel Rio (UCL), Paul Waldron (Orange) and Professor Paul Reynolds (France Telecom R&D UK), and the resources of the Orange Fraud and Revenue Assurance Online team space. This work is supported by the EPSRC.

References

[1] "Fraud." West's Encyclopaedia of American Law. The Gale Group, Inc, 1998. *Answers.com* 8 Jun. 2006. http://www.answers.com/topic/fraud

[2] Telecommunications (Fraud) Act 1997, Chapter 4, ISBN 0 10 540497 7

[3] GSMA Certified Fraud Training Programme. GSM Association. *GsmWorld.com* 27 Jun. 2006. http://www.gsmworld.com/fraudtraining/index.shtml

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. RFC 3261, Internet Engineering Task Force, June 2002.

[5] 3GPP. Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1, (Release 8), TS 22.228 V8.0.0 (2006-06), 3rd Generation Partnership Project (3GPP), June 2006.

[6] Unified Modelling Language. Object Management Group. *Uml.org* 30 Jun. 2006. http://www.uml.org

[7] ISO/IEC, "ISO/IEC 10746-1 Information technology – Open Distributed Processing – Reference Model: Overview", 1998.