Fraud Detection for Next-Generation Networks

Name of company/ies submitting case study:
University of Deusto
Web links to company/ies submitting case studies:
http://www.deusto.es
http://www.fundacion-deusto.deusto.es/

Name of author(s):
Igor Ruiz-Agundez
Yoseba K. Penya

Authors' email address(es):
igruiz@tecnologico.deusto.es
ypenya@tecnologico.deusto.es

Contact for further information (to be posted on TM Forum website):
Igor Ruiz-Agundez (igruiz@tecnologico.deusto.es)

Applicable TM Forum technical areas
IPDR

Applicable Industry Areas:

VIEWPOINT:	
X	Service provider perspective
X	Software vendor perspective
	Hardware vendor perspective
	System integrator perspective
SERVICES:	
	Voice
X	Video
X	Data
X	VoIP
X	IPTV
	VPN
X	Content

NETWORK TECHNOLOGIES:	
	Mobile GSM/GPRS
	Mobile CDMA/EVDO
	Mobile Edge/UMTS
	ATM
	SONET/SDH
	MPLS
	Ethernet
	Frame Relay
X	Converged network
	Cable
	Satellite
	Broadband
	Fixed Line
	DSL
X	IP
	WiFi/WiMax

CASE STUDY SUMMARY:

Next-Generation networks (NGN) introduce new services and infrastructures, posing a new scenario of risks and security issues. Together with classical security risks that are adapting to NGN's special conditions, brand new threats will emerge. In order to face these risks, Fraud Management Systems (FMS) need to evolve to adequately tackle such new challenge.

This Case Study describes a fraud management system implementation deployed for VoIP and other IPDR services as defined in their respective service specifications. The FMS is based on misuse detection techniques that can be combined with other complementary fraud detection techniques in order to guarantee the stability and the revenues of the provided services.

FULL CASE STUDY:

- **Business Problem to be solved:**

In order to guarantee the legitimate use of the provided services, service providers have to face many security risks such as classical security attacks (e.g. denial of service (DoS), sniffing, spoofing or spam) or brand new threats. Standing out in this latter group, fraud is considered to be the most harmful.

Fraud from employees, consumers, third-party, computer crime, insurance or financial fraud increases every year. More accurately, in our target area, telecommunications, the increment has reached the 52% from 2003 to 2005.

With the objective of tackling these risks, Fraud Management Systems (FMS) detect and analyze fraud and suggest counteractions. Traditional FMS, however, are service specific and depend on the underlying network infrastructure. As NGN introduce new services and infrastructures, FMS need to adapt themselves too.

- **Working towards a solution:**

The University of Deusto has worked in information security and fraud management in different scopes, from the foundry industry failure detection to information security consulting.

Dealing with fraud is a very complex task mainly due to its transversal nature to the operators' structure. Traditional fraud techniques are evolving and adapting to the new network infrastructure. We have to consider them because the basic ideas remain despite the underlying technology. Moreover, we have to focus on the specific risks around the NGN.

Deception in telecommunications includes subscription frauds, where the cheater accesses the services without being subscribed. Users can also suffer line or identify theft, being charged for services used by others. Telecommunication operators can oversee users that exceed their download quote and rate performing illegal service redistribution, sometimes for an economic profit. Finally, cloning or unauthorized access to services may lead to compromising privacy.

Technology and security advance in parallel; this reason complicates foreseeing future risk scenarios and, consequently, the ways to face them. As the technology evolves, so do the security needs. In this way, we consider that the security risks can be catalogued according to their effect on the system or the client.

For instance, the system may suffer a service continuity interruption, ranging from attacks as Denial of Service (DoS) or physical attacks to the network or service provider hardware. Moreover, there may be abuses based on logical attacks such as insufficient validation of the services or abuses of functionality (using a service for not expected task). This latter thread is related to information disclosures due to predictable resource location, information leakage, or directory indexing.

Furthermore, intrusions may compromise network systems by executing unauthorized commands, taking advantage from architectural or design vulnerabilities. Privacy of the clients or the stored data may be exposed too by several techniques like sniffing, spoofing, spamming or phising. Access to services can be bypassed with authentication attacks (e.g. brute force or password inference) or with authorization attacks (e.g. credential prediction or insufficient authorization schemes).

Note that we focus here on the possible risks that fraud can cause to service providers, customers and stakeholders. Fraud is defined as *"a deliberate act of obtaining access to services and resources by false pretences and with no intention of paying"*.

Anyway, the most common types of fraud on telecommunications are subscription fraud and identity theft. After those, voice mail fraud and calling card fraud prevail. The analysis of the different fraud techniques points out that the tendency is a convergence of the fraud, which increases the complexity of its detection.

Fraud Management Systems have proved to be a suitable tool to detect fraud in different networks with diverse techniques: self-organizing maps (SOM), general data mining or rules. Nevertheless, there is none to our knowledge that works on fraud detection for VoIP services in NGN with use cases.

- **Solution:**

The FMS meets the IPDR architecture as shown in Fig.1. It is allocated in the business support system and receives data in IPDR format for its analysis. When the system receives an IPDR as an input data the fraud detection process starts. Each IPDR is sent to a rule engine containing expert knowledge about fraud in order to detect a possible violation.

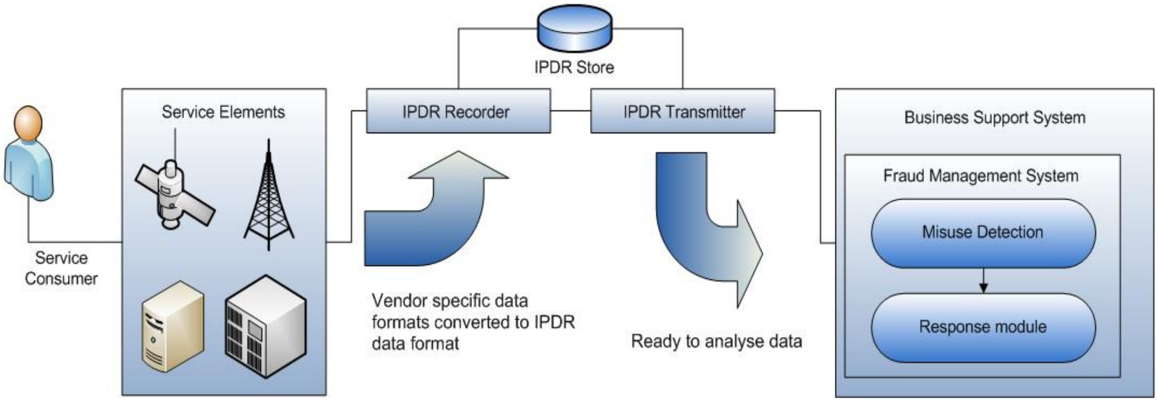

Fig. 1 Fraud Management System for IPDR

The FMS is allocated in the business support system and receives data in IPDR format for its analysis. Once the FMS receives an IPDR as an input data the fraud detection process starts. Each IPDR is sent to the rule engine that contains the expert knowledge about fraud in order to detect a possible violation using misuse detection techniques. If the FMS detects a possible fraud, it reports the incident to the response module. This final module can trigger a fraud notification alarm to the system operator or it can block all the present and future connections of a suspicious client.

The skeleton of our system is based on software agents (say small autonomous software programs). More accurately, this software agent uses current perceptions from the sensors as input, returning an action to the actuators as an output. Moreover, it selects the most suited action to perform on the basis of the current perception, the current IPDR. We can consider this agent a simple reflex one because its decision making is based only on the current input data.

Our system uses an existing framework, Drools, that provides a full set of tools to define our knowledge base. Drools is a Rule Engine that uses a rule-based approach to implement an expert system and is more correctly classified as a production rule system.

The production rules from a two-part structure that uses First-Order Logic for knowledge representation (which is sufficiently expressive to represent a good deal of common-sense knowledge). They include a condition clause and an actions clause that will trigger when the conditions are true. In our experiment, the responsible of defining the rules is an expert in the domain of the security in telecommunications. These rules are defined with previous knowledge and are limited to the scope of the misuse detection in this specific domain. Anomaly detection, or other boundary cases, is not under the field of this experiment.

- **Results:**

We introduce a misuse-detection-based system to detect fraud on Voice over IP and other services on Next-Generation Networks, in order to improve fraud management systems for NGN. We believe that detecting potential security risks contributes to the deployment of these networks by providing extra stability. Besides, the investments on infrastructures and development by telecommunication operators are stepped up.

We believe that misuse detection is the best approach to build a fraud management system that controls these risks. Our analyses show that this paradigm works and is able to react when a fraud attempt occurs.

This reactive capacity provides a faster detection of deception use of services. This reaction time is essential for a service provider for taking the necessary countermeasure guaranteeing the integrity of its services.

These categories will be used for placement on the TM Forum website and to make your case study retrievable by the TM Forum website search engine:

Applicable TAM Application Framework Categories:

Market/Sales	
	Campaign Management
	Channel Sales Management
	Corporate Sales Management
Product Management	
X	Product Performance Management
	Product Catalog Management
	Product Strategy/Proposition Management
	Product Lifecycle Management
Customer Management	
X	Customer Information Management
	Customer Self Management
	Customer Contact, Retention & Loyalty
X	Order Management
	Quotation Engine
X	Customer QoS/SLA Management
	Customer Service/Account Problem Resolution
X	Customer Billing Management
X	Invoicing
X	Collections Management
X	Bill Formatting
	Receivables Management
Service Management	
X	Service Specification Management
	Service Inventory Management
X	Service Configuration Management
	Service Design/Assign
	SLA Management
	Service Problem Management
	Service Quality Monitoring and Impact Analysis
	Service Performance Management
	Service Rating/Discounting Management

Resource Management	
	Workforce Management
	Resource Specification Management
	Resource Inventory Management
	Resource Design / Assign
	Resource Provisioning / Configuration
	Resource Logistics
	Resource Testing Management
	Resource Activation
	Resource Planning / Optimization
	Resource Domain Management (IT Computing, IT Application, Network)
	Resource Performance Monitoring / Management
	Resource Problem Management
	Correlation & Root Cause Analysis
	Resource Status Monitoring
	Resource Data Mediation
	Arbitrage Management
	Voucher Management
X	Billing Data Mediation
X	Real-time Billing Management
Enterprise Management	
X	Revenue Assurance Management
	HR Management
	Financial Management
	Asset Management
X	Security Management
	Knowledge Management
X	Fraud Management
Supplier/Partner Manager	
	Partner Management
	Supply Chain Management
X	Wholesale/Interconnect Billing Application