

ROC® Fraud Management for DTH and IPTV Service



Concept Note on ROC Fraud Management for DTH and IPTV Service

Introduction

ROC Fraud Management System is built to drive fraud prevention by eliminating known frauds, reducing free run time, augmenting internal controls and through continuous FM process improvement. ROC Fraud Management has the ability to detect fraud types associated with TV and Video services such as IPTV, Satellite, Cable and Terrestrial broadcast. These Service Providers support one or more of the following delivery types:

- On-demand Streaming (near real-time delivery)
- On-demand Download (freedom to watch any time afterwards)
- Broadcast Streaming
- Broadcast download

There are currently three primary types of technologies used to protect video application intellectual property (IP) rights: content protection systems; conditional access systems; and digital rights management. Exchange is secured most commonly through smartcard technology.

The various underlying charging model for such services may be:

- Pay-per-view Per-event;
- Pay-per-view based on duration;
- Pay-per-view based on volume (size)
- Subscription models;

Pay on demand could be on-line pay-per view, or prepayment for services. Hybrid models are also common, and whilst registration is an integral part of subscription-based services, PPV services may be subscription-based or anonymous.

Any fraud management capabilities are entirely dependent on the nature of information made available to the system. Typical information types include:

Subscription information and credentials

- personal info
- banking info
- payment history
- etc

Usage (event) info:

- Subscriber id
- Location(?)Volume
- Time/date
- Duration (session time)
- Service type (e.g. film)
- Service Genre (e.g. pornographic)
- Service identity (film title)
- Cost

ROC Fraud Management Capabilities

ROC Fraud Management provides a one stop solution to handle the fraud threats that affect TV and video services. ROC Fraud Management's capabilities to tackle fraud are highlighted with the help of few fraud scenarios

Concept Note on ROC Fraud Management for DTH and IPTV Service

Fraud Scenarios

Subscription Fraud

Subscribers may provide wrong information like invalid/stolen identity details, stolen/compromised credit cards etc. for subscribing the services with the intention of accessing services and not paying the bills. Stolen Set top boxes/smart cards/logins could be used for accessing the services causing the loss to operator or to one of the genuine subscribers of operator.

ROC Fraud Management countermeasure: Pre-check to detect re-offending fraudsters and bad debtors

ROC Fraud Management countermeasure: Hotlist username, IP address, or MAC address.

Precheck functionality of ROC Fraud Management runs multiple checks on new subscription and against blacklists and identifies fraudsters based on phonetic match, exact match and combination matches.

Hot listing of fraudsters/ credit cards/ equipments identifies fraudsters quickly.

Scenario: Detect the subscribers who have not subscribed to services are being able to access services. For example users don't have subscription but still are able to download videos on demand.

ROC Fraud Management countermeasure: Use invalid subscriber events.

ROC Fraud Management countermeasure: eFingerprinting to spot changes in regular genres/habits.

ROC Fraud Management patent pending eFingerprinting technique captures detailed subscriber behavior (calls, actions, locations, etc) and match against a hotlist of previously recorded fraudster's Fingerprints without relying on any subscriber credentials (name, address, etc)

Dealer/Sales Fraud

Scenario: Preconnection and commission fraud.

ROC Fraud Management countermeasure: Low/no usage rules to detect Dealer/Sales commission fraud

Service violation

Scenario: use of service not subscribed to.

ROC Fraud Management countermeasure: Invalid subscriber detection

Abuse of 'Subscription' i.e. gaining access to content outside that specified in the contracted 'service package' could happen in the form of Chipping' - This involves the attachment of a pre-programmed microprocessor to a Set Top Unit (STU) control chip or the alteration of the STU's own chip by software techniques to enable full network service and pay on demand services to be obtained when only a basic package has been contracted.

Another method of gaining this access is via the use of a 'cube'. This is a device which connects to the back of a STU. It overrides the signal from the head end and allows access to the full service package.

Usage Fraud

(For Pay on Demand (e.g. Pay-Per View) Services)

Scenario: High PPV usage

ROC Fraud Management countermeasure: Usage based rules e.g. excessive high use

Concept Note on ROC Fraud Management for DTH and IPTV Service

Fraud Scenarios

Scenario: high PPV usage on an account with other services that have high other types of usage

ROC Fraud Management countermeasure: either use a smart pattern or cumulative value based rule
Cable providers have been monitoring high PPV, or high On Demand.

Scenario: High volume high risk titles

ROC Fraud Management countermeasure: Usage based rules e.g. excessive high use

Scenario: High risk/high volume 'adult' rated titles.

ROC Fraud Management countermeasure: Usage based rules e.g. excessive high use

Scenario: Unauthorized access and modification of premium content

ROC Fraud Management countermeasure: Unauthorized service use

Stolen Equipment

Scenario: Stolen or compromised end-user equipment.

ROC Fraud Management countermeasure: Hotlist - Use/registration of stolen identity (i.e. equipment)

ROC Fraud Management countermeasure: RoC to spot changes in regular genres

Cloning

Scenario: Cloned Smartcard/Equipment

ROC Fraud Management countermeasure: detection using overlap/velocity (need a location or secondary id such as overlapping use on distinct IP addresses)

ROC Fraud Management countermeasure: RoC to spot changes in regular genres/habits

Scenario: Password/PIN theft/compromise/sharing

ROC Fraud Management countermeasure: overlapping calls/velocity

ROC Fraud Management countermeasure: RoC to spot changes in regular genres/habits.

Scenario: Cloning smart cards and distributing 'free access' cards – worse than cloning.

ROC Fraud Management countermeasure: Rules possible if server side verification is involved

Scenario: Modified 'all-access' smart cards

ROC Fraud Management countermeasure: Rules possible if server side verification is involved

Hacking

Scenario: Illegal service access attempts

ROC Fraud Management countermeasure: Smart-patterns to detect combinations like few unsuccessful logins then continuous high usage

Scenario: Modify cards to obtain additional services

ROC Fraud Management countermeasure: Service violation event based on server side usage data

Scenario: Break security protection measures (technical fraud)

ROC Fraud Management countermeasure: Rules based on Authentication logs on network elements

Concept Note on ROC Fraud Management for DTH and IPTV Service

Reselling

Scenario: Overriding DRM and selling-on downloaded content

ROC Fraud Management countermeasure: Customized Reports on secondary account by dealer area etc.

Ghost Accounts

Scenario: Intruders or internal abusers might try to control the provisioning infrastructure or the billing infrastructure as part of a fraud attempt either by creating "ghost" accounts or changing the entries on the billing system.

ROC Fraud Management countermeasure: Look for service discrepancies – i.e. unauthorised service type.

Content Theft

Scenario: Trojan horses to steal access to content. Subscribers might inadvertently install software that allows intruders to gain access to content and even request VOD (Video on Demand) using the subscriber's account. Need AV and regular updates to S/W.

ROC Fraud Management countermeasure: High usage rules on VOD usage logs

Scenario: Capture (extract) content and re-distribute for free (hacker) or for sale (fraudster)

ROC Fraud Management countermeasure: High download rules on usage logs

Scenario: Redistribute broadcast stream to others

ROC Fraud Management countermeasure: High download rules on PPV usage logs

Internal fraud

Scenario: many of the typical scenarios are possible.

ROC Fraud Management countermeasure: Internal affairs Module, rules based on audit logs of internal systems

The internal affairs module in ROC Fraud Management monitors activity associated with the customer's corporate systems – storing employee data, taking in system log files, and supporting rules to detect suspect system modifications and unusual employee activity/behavior.

Credit/Debit card fraud

Scenario: Policy controls for stolen/compromised card use. Most usual scenarios occur.

ROC Fraud Management countermeasure: In-line transaction controls.

ROC Fraud Management's transaction fraud module performs various in line checks, advanced analytics on transaction data and provides custom reports which help check fraud at the transaction stage.

Scenario: Phone up and pay, Internet payment, etc. With or without subscription/registration. Unregistered card payment issues. Card not-present issues

ROC Fraud Management countermeasure: High card use, high aggregate card spend, high account spend, hot listed card use, card use across multiple accounts, multiple cards used on single account.

DoS

Scenario: Quality of service degraded. In the case of viruses and worms, a disruption can be caused to the service either by saturation of the networks or by crashing the network elements (e.g. provisioning, billing) and end points. VOD impact on revenue

ROC Fraud Management countermeasure: rules based on authentication/paging logs

Concept Note on ROC Fraud Management for DTH and IPTV Service

SPIV

Scenario: SPAM over IPTV - SPIV unsolicited adverts etc. if not authenticated by end user equipment.

ROC Fraud Management countermeasure: high volume downloads in short space of time. Do event records like this exist?

AIT (Artificial Inflation of Traffic)

An operator needs to ensure that where content is provided to the customer the demand for the content is genuine. Content providers will often work on a revenue share arrangement akin to a premium rate service model. Due to this the content provider has an incentive to ensure high volumes of traffic are passed to their service in order to receive the highest revenues. This may lead to content providers artificially inflating traffic to their own content.

ROC Fraud Management countermeasure: rules based on hotlists and high usage of premium services

Note: The countermeasures indicated are at higher level and generic in nature. Subex can assist in further defining the countermeasures based on specifics.

About Subex

Subex Limited is a leading global provider of Business Support Systems (BSS) that empowers communications service providers (CSPs) to achieve competitive advantage through Business Optimization - thereby enabling them to improve their operational efficiency to deliver enhanced service experiences to subscribers.

The company pioneered the concept of a Revenue Operations Center (ROC®) – a centralized approach that sustains profitable growth and financial health through coordinated operational control. Subex's product portfolio powers the ROC and its best-in-class solutions such as revenue assurance, fraud management, credit risk management, cost management, route optimization, data integrity management and interconnect / inter-party settlement.

Subex also offers a scalable Managed Services program and has been the market leader in Business optimization for four consecutive years according to Analysys Mason (2007, 2008, 2009 & 2010). Business optimisation includes fraud, revenue assurance, analytics, cost management and credit risk management. Subex has been awarded the Global Telecoms Business Innovation Award 2011 along with Swisscom for the industry's first successful Risk Reward Sharing model for Fraud Management.

Subex's customers include 16 of top 20 wireless operators worldwide* and 26 of the world's 50 biggest# telecommunications service providers. The company has more than 300 installations across 70 countries.

*RCR Wireless list, 2010

#Forbes' Global 2000 list, 2010



www.subex.com

Subex Limited

Adarsh Tech Park,
Devarabisanahalli,
Outer Ring Road,
Bangalore - 560037
India

Phone: +91 80 6659 8700
Fax: +91 80 6696 3333

Subex Inc.

12101 Airport Way,
Suite 300 Broomfield,
Colorado 80021
USA

Phone: +1 303 301 6200
Fax: +1 303 301 6201

Subex (UK) Limited

3rd Floor, Finsbury Tower,
103-105 Bunhill Row,
London, EC1Y 8LZ
UK

Phone: +44 20 7826 5420
Fax: +44 20 7826 5437

Subex (Asia Pacific) Pte. Limited

175A, Bencoolen Street,
#08-03 Burlington Square,
Singapore 189650

Phone: +65 6338 1218
Fax: +65 6338 1216