International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 16

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.800-X.849 series – Supplement on architectural systems for security controls for preventing fraudulent activities in public carrier networks

ITU-T X-series Recommendations – Supplement 16

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Supplement 16 to ITU-T X-series Recommendations

ITU-T X.800-X.849 series – Supplement on architectural systems for security controls for preventing fraudulent activities in public carrier networks

Summary

Supplement 16 to the ITU-T X-series Recommendations describes a methodology for evaluation systems of security controls for preventing fraudulent activities, and criteria for selection of these systems, with regard to architectural characteristics of communications service provider (CSP) networks at their present-day level of development. The Supplement includes technical methods for addressing security controls and estimating losses caused by fraudulent activities, and also provides guidelines for the exchange of information related to fraudulent activities.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 16	2012-09-07	17

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 16 to ITU-T X-series Recommendations

ITU-T X.800-X.849 series – Supplement on architectural systems for security controls for preventing fraudulent activities in public carrier networks

1 Scope

This Supplement describes an architecture of security systems for prevention of fraudulent activities in public carrier networks. This Supplement describes an example architectural model that provides technical methods to:

- provide guidelines for security features on internal (end-to-end) service provisioning, assurance and billing processes;
- address security controls for preventing external fraud attacks affecting public carriers' customers and partners;
- estimate losses (for example, QoS, service degradation, etc.) caused by fraudulent activities.

This Supplement also provides guidelines for information exchange related to fraudulent activities.

While it is clear from the ITU Constitution that all implementations, based on ITU Recommendations, shall comply with national laws, policies and regulations, because this Supplement suggests using something similar to lawful interception techniques to combat fraud, implementers should be especially sensitive when implementing this Supplement to ensure that the resultant implementation complies with national laws, policies and regulations.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 database management system (DBMS) [b-ISO/IEC TR 10032]: Is a set of computer programs of general and specific functions that controls the creation, maintenance, and the use of a database.

3.1.2 operation support system/business support system (OSS/BSS) [b-ETSI TR 102 647], [b-ETSI TS 188 001], [b-ETSI TR 188 004]: Computer systems for complete or partial automation of activities of communication service providers.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 confidential information: Information to which access is restricted by law or regulation, and which is a commercial, official or personal secret guarded by its owner.

3.2.2 counterpart: One of the contracting parties.

3.2.3 customer relationship management system (CRM): Corporate information system, designed for automation, organization and synchronization of a telecom operator's business processes, particularly sales, marketing and customer relationship improvement, and storing of all relationship history.

3.2.4 documentary information (document): Information recorded on a material object (hereinafter referred to as material medium) with document entries allowing identification of the information or, in legally stipulated cases, its material medium.

3.2.5 fraud attack: A telco fraud committed by a telco fraudster within a particular period of time.

3.2.6 information constituting a trade secret: Information is deemed a trade secret if it is actually or potentially valuable by virtue of its being unknown to third parties and inaccessible on legal grounds. Its owner takes measures for its protection.

3.2.7 invoicing: Telecom operator billing subsystem for invoice preparation, discount application and invoice aggregation into a single bill.

3.2.8 mediation: A system converting (accumulating, filtering, modifying and correlating) source data on telecommunication network usage into data that can be interpreted by communication service providers' OSS/BSS.

3.2.9 owner of confidential information: An entity that generated confidential information or, by force of law or contract, obtained the right to allow or deny access to such confidential information.

3.2.10 rating: The calculation of charges for the customer that can be performed without knowledge of the aggregate. Rating enables different payment schemes, and contains databases with tariffs as well as charge-application schemes.

3.2.11 recycle: A system that takes part in traffic processing and stores data that are not included in the telecom operator's client bills for certain reasons. Such reasons are: failure to anchor xDRs to a specific subscriber, lack of tariffs for service in question, and xDRs of a format different from that processed by the OSS/BSS.

3.2.12 restricted access mode: Legal, managerial, technical and other measures taken by the owner of confidential information for its protection.

3.2.13 telco fraud (fraud in international telecommunication networks): Damage to telecommunication companies or to the public; it is earning illegal profit through abuse of confidence or deception in international telecommunication networks services, including improper use of numbering resources, addressing and identification.

Grounds: illegal operations control in networks related to service companies and subscribers of different jurisdictions can only be conducted on the authority of an international treaty, such as International Telecommunication Regulations, and only provided that relevant national legislations are harmonized.

3.2.14 telco fraudster: A party (person or organization) in which interactions with a service provider can be categorized as telco fraud.

3.2.15 unauthorized disclosure of confidential information: Action or inaction which results in confidential information becoming known to third parties in verbal, written or other forms (including via technical means) without the consent of the information owner.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

BSS Business Support System

CRM Customer Relationship Management System

CSP Communications Server Provider

DBMS Database Management System

FMS Fraud Management System

ICT Information and Communication Technology

OSS Operation Support System

PIN Personal Identification Number

PRS Premium Rate Services

SIM Subscriber Identity Module

xDR Call/IP Detail Record

5 Conventions

The term "communications service provider" as used here includes all communications service providers, including telecommunication operators, telecommunication companies and telecom carriers.

6 Overview

Fraudulent activities by employees, clients and business partners (e.g., communication service providers) in the telecommunication sector exist on the fixed, cellular mobile, cable and satellite communication networks, regardless of the underlying communications technology.

The most widespread fraudulent activities are the organization of unapproved public telephone booths, gaining revenue by means of theft of PIN-codes, of telephone cards, or breaking of algorithms of their generation, cloning of cellular mobile telephone SIM cards and use of false identification to register in a communication network.

One of the most serious kinds of fraudulent activities is action taken by communication service providers' employees to deliberately activate an unpaid telecommunication service.

Fraudulent activities are classified as follows:

- internal methods, implemented by employees of a communication service provider (e.g., to change rating systems or undercharge counterparties traffic sale), deliberately take advantage of technical defects in equipment and/or errors in OSS/BSS interconnection;
- external methods, implemented by communication service providers' clients or counterparties (illegal access, breaking into an automatic telephone exchange, false authentication).

Formal definitions of telco fraud are outlined in clause 3.2.13, telco fraudster in clause 3.2.14 and fraud attack in clause 3.2.5.

There are six main types of fraud.

a) **Technical fraud** consists of any activities undertaken by outside employees, clients or counterparts of communication service providers, to make fraudulent usage of service providers' services without proper payment, taking advantage of the technical defects of a telecommunication network and/or shortcomings of OSS and BSS interconnection.

   Types of technical fraud are related to:

   - technical issues in implementation of telecommunication network standards and specifications;
   - telecommunication vendors' respect and implementation of standards in equipment and software;
   - design features of the service provider's telecommunication network during the creation and development of the network.

Examples of technical fraud are:

- call redirection and forwarding fraud are fraudulent usage of specific call-forwarding capabilities of the cellular mobile network equipment to make voice calls, or send messages, which are due to be paid by an unaware customer who has those services enabled;
- voicemail fraud is fraudulent usage of cellular mobile network equipment voicemail capabilities to make voice calls or send messages that are due to be paid by an actual customer with a contract in which those services are allowed.

b) **Payment fraud** is based on a counterfeit contract signed using illegitimate or stolen documents, modified customer details or false identity information. This kind of fraud makes use of communication provider services and resources with the prior intention of not paying for them. Payment fraud is based on the use of sham or stolen debit or credit cards and of their PIN codes, and false cheques for payment of service provider bills.

Examples of payment fraud are:

- usage of illegitimate or stolen documents or identification information with the purpose of signing a pseudo-legal contract with a service provider, and using its services and resources;
- usage of a fraudulent credit or debit card with the purpose of making payments of service provider bills without the permission or authorization of the lawful holder of the credit or debit card;
- usage of sham cheques with the purpose of making false payment from an account in deficit, or an account for which the fraudster does not have legal permission to access.

c) **Service provider partner and dealer fraud** is based on commercial activity involving third parties (usually resellers) that incurs revenue losses for the communication service provider. Such fraud is usually aimed at gaining unlawful preferences or dealer commissions from the service provider.

d) **Business fraud** is based on the use of:

- services of the cellular mobile operator outside the home network, with no intention of paying for these communication services (fraud related to a subscriber being in a roaming state);
- telecommunication value-added services or voice services that provide the subscriber with different kinds of information or content for an additional fee (PRS fraud);
- stolen SIM card, pre-activated kits for the use of mobile communications, mobile phones, including property obtained through theft, robbery or other illegal activities, but excluding the acquisition of property through the unauthorized use of credit cards.

e) **Internal fraud** is based on the intentional use by employees of a telecommunications operator of their knowledge of vulnerabilities in the technology and business processes of CSP for personal gain or profit or damage to the reputation of the company.

f) **Prepaid fraud** is based on any use of a pre-paid product that results in loss of income for the operator, e.g., unauthorized use of a prepaid subscriber's account. Prepaid fraud includes any case where fraud, using technical or other errors or network vulnerabilities, enables the use of prepaid services without payment.

7 Architecture of security systems for the prevention of fraudulent activities in public carrier networks

The technical method used to take actions to counter fraudulent activities is divided into two groups from the viewpoint of automation level:

- ICT dependent;
- automated systems and modules.

Technical methods of fraud prevention often fall within the area of responsibility of the ICT department of telecom operators. Consideration should be given to accomplishing activities in this area based on formal requests. The ICT department in turn responds with a set of documented events related to fraud activities.

Fraud management systems (FMSs) are the basic automated resource on revealing and preventing fraudulent activities.

FMS is the hardware-software complex that carries out constant monitoring, conducts the analysis and estimation of all events occurring in a communication service provider's network, and estimates the likelihood that the given event is fraudulent.

FMS allows the automation of processes of identification of fraudulent activities, the investigation of the facts on fraudulent activities and formation of statistical reporting.

This Supplement is intended to describe FMS features, and handling of fraud prevention methods applicable to switched telephone networks, both packet-based and line-switched.

Static slice of FMS for a given moment includes the following.

- Application architecture – functional and component structure of the information system;
- Data architecture – the means of interconnecting systems and data storage;
- Equipment architecture – hardware used.

Application architecture includes:

- Monitoring objects – monitoring objects depends on network types and can be A-numbers, IP-addresses, trunk group names, ports, etc.
- Support of various types of communication networks – capability of processing data according to communication network types.
- Estimation of prevented revenue loss.
- The kinds of fraudulent behaviour, which depend on the communication network type.
- Support of subscriber profiles and subscriber groups.

Data Architecture constitutes the means for FMS to communicate with external OSS/BSS of a telecom operator's business processes and operations, as well as formats and data storage methods.

FMS data contain detailed records (xDRs) generated by telecom servicing equipment or signalling links monitoring equipment in binary or text format.

In production application of FMS the telecom operator will connect with the following OSS/BSS.

- Mediation – for the uploading of xDRs into FMS, integrity checks and data storage.
- CRM – for incorporating and linking raw xDR data to customers.
- Rating – for exporting tariffs to provide an approximate calculation of customer charges.
- Invoicing – for matching the processed FMS data against bills presented to a telecom operator's clients.

Hardware architecture includes:

- mediation;

- application server with fraud protection functionality;
- reporting server.

It may also include a hardware and software complex for monitoring of signalling lines. This component collects data and cannot influence the telecommunications network.

Generally, a probe system decodes signalling protocols in real time. The system is connected to a switch port of the telecom carrier, where all signalling data to be analysed is collected. The system provides services for obtaining data processing results. The probe system includes a database to store the procession results.

The system has the following parameters:

- probing interface;
- supported protocols;
- average/peak traffic (number of connections per second);
- average volume of attribute data (in MB);
- archive storage time (in days);
- storage format (formatted files of attributes with data autorotation);
- attributed database update period (in seconds).

FMS, as hardware and software complexes, often share one or more of the following characteristics:

- Performance – The performance of FMS is measured by the number of xDRs processed in a given period of time.
- Continuous operation of FMS – This issue is concerned with evaluation of the loss and restoration of xDRs entering the FMS.
- User interface requirements.
- Security system management.

Figure 1 demonstrates the work of FMS on the telecommunications network of a communication service provider.

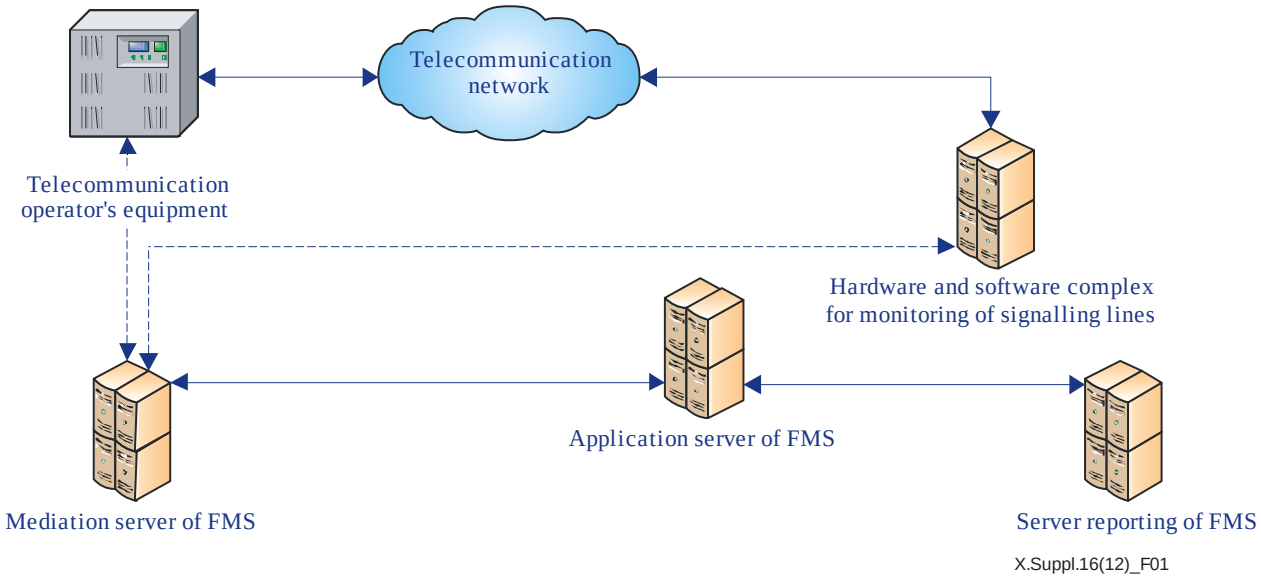

Figure 1 – The work of FMS on the telecommunications network of a telecommunications operator

8 Technical methods to provide guidelines for security features on internal (end-to-end) service provisioning, assurance and billing processes

There is a process that allows interaction between different departments of a communication service provider within the framework of one type of service.

Technical methods to provide guidelines for security features on internal (end-to-end) service provisioning are expressed in FMS capabilities to match different types of data streams.

When FMS is introduced to a given telecommunications service rendering process, key nodes between the point of client connection hardware and the point of invoicing are chosen and internal data are matched against reference data received independently from a telecommunication network.

This allows countering fraudulent behaviour such as irregular use of link channels, equipment failures, operation failures/the company's OSS/BSS interface failures, abuse of position by altering service billing parameters such as start and end time of billed calls, etc., which are indicators of internal fraudulent behaviour.

Figure 2 demonstrates the work of FMS for the following case of switched telephone networks, both packet-based and line-switched services.

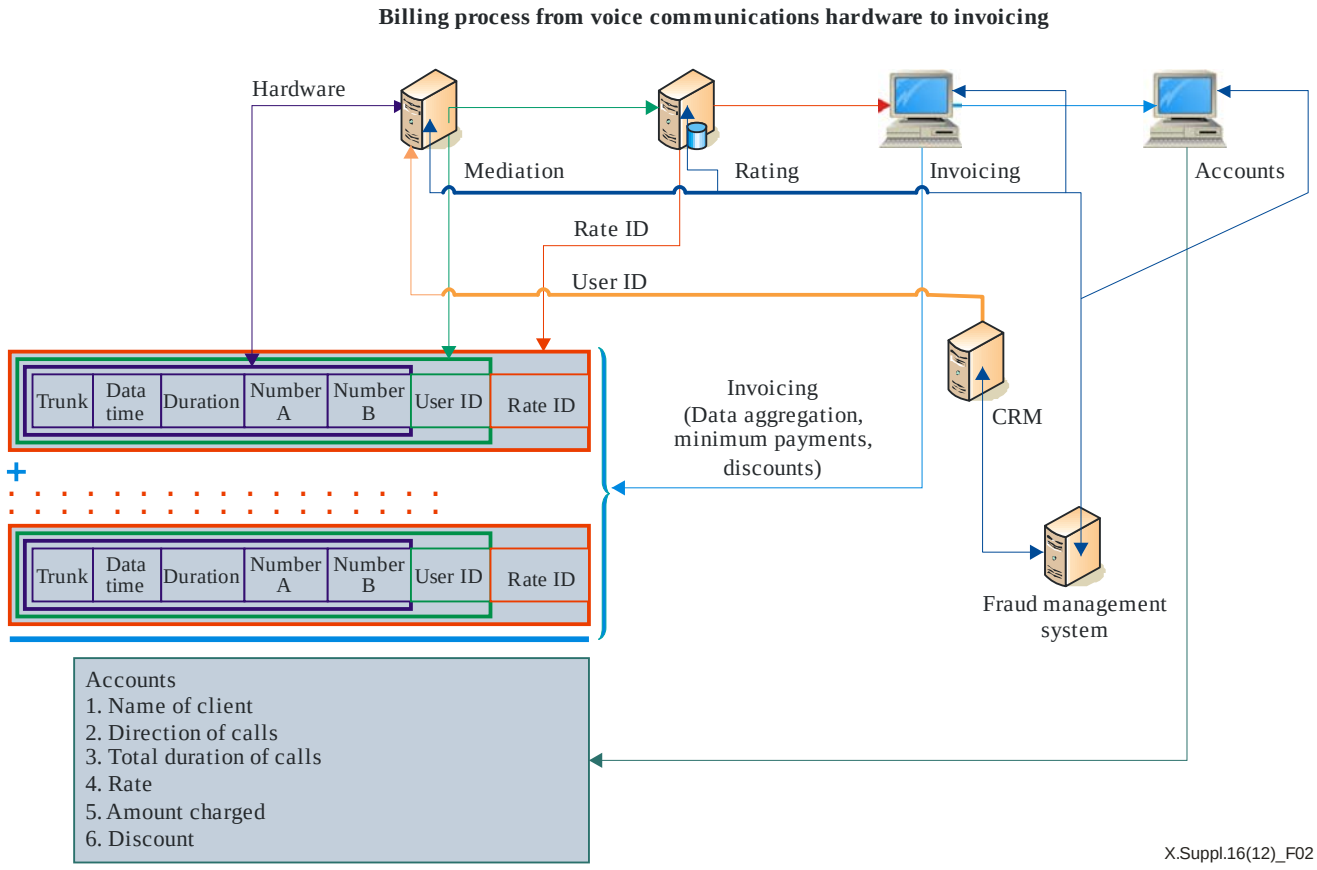

Figure 2 – Billing process from voice communications hardware to invoicing

As its reference data source, FMS uses either data generated by the hardware or data generated by a hardware and software complex designed for monitoring of signalling lines.

This hardware and software complex allows non-intrusive connection to the voice network of a telecom operator and data collection in real time.

Implementation of such hardware and software complexes provides initially accurate data on calls and, consequently, enables matching it against a telecom operator's OSS/BSS results.

The generated data are standardized with parser programs that are included in mediation FMS software.

This approach allows internal fraudulent behaviour to be opposed by matching telecoms network data against mediation data of a telecom operator.

Additionally, a telecom operator's billing department is aided in the allocation of entries from the recycle system.

After the data are processed at mediation, and CDRs are attributed to proper subscribers (guiding), the data are fed to the rating system. At this point the guiding process may be checked for accuracy (to ensure that the calls are correctly attributed to the operator's clients).

At the rating point the FMS allows pseudo rating based on mediation FMS data and rate data from the paper medium.

It continues along the chain of data processing servers, as shown in Figure 2.

Thus, the resources of FMS allow the building of a chain of verifications at points of key importance to enhance billing accuracy.

The FMS used in the discussed example is a hardware and software complex with the following functions:

- basic mediation;
- matching polytypic data flows;
- pseudo rating;
- reporting.

9 Technical methods to address security controls for preventing external fraud attacks affecting public carriers' customers and partners

The FMS function implements technical methods to address security controls for preventing external fraud attacks on the basis of analysis of the behaviour of communications service providers' clients/counterparts, by means of construction of subscriber profiles and their analysis, with the following purposes:

- revealing subscribers whose profiles differ significantly from others in their group;
- revealing subscribers who have sharply changed their behaviour;
- modelling subscriber behaviour;
- revealing subscribers with consumption of services falling into pre-set intervals;
- revealing the connection between two subscribers;
- splitting subscribers into clusters according to service consumption.

Figure 3 demonstrates this function in detail for voice telecommunications services with analogue and digital time-division multiplexing and also voice over IP communications services.

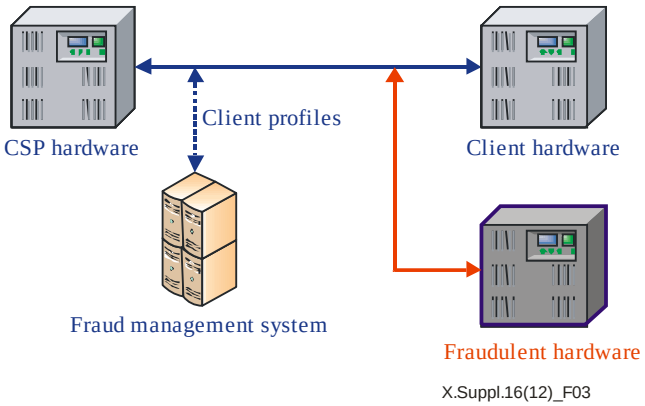

Figure 3 – Irregular connection of outsider telecom equipment

The end user/the counterpart of a communication service provider makes calls during a certain period of time, creating a subscriber profile – a set of geographical directions, frequencies and call durations to these destinations. Malicious outsiders, having obtained access to the equipment of the client (client/counterpart hardware) or having connected in parallel, make calls instead of, or in parallel with, the client/the counterpart. As a result, the profile of the subscriber starts changing, which FMS reports to the appropriate divisions of the telecom carrier in real time. Thus, before the client/counterpart of the telecom operator challenges their invoice at the end of the reporting period, FMS warns the communications operator in advance about possible fraudulent behaviour.

10 Fraud loss estimation

Fraud detection and elimination imply accurate evaluation of the financial impact of this function's operation from the viewpoint of detected and prevented financial loss. Different types of evaluation models may be used according to the type of fraud.

- Evaluation of discovered loss: i.e., the loss that was suffered by a telecommunications operator, which it would continue to suffer without fraud prevention functionalities.
- Evaluation of prevented loss: i.e., the loss that was prevented and that can be considered as recovered.
- Evaluation of indirect loss for those types of fraud that cannot be financially measured: e.g., fraud tarnishing the image of a trademark, negatively influencing the trust and loyalty of clients and others.

Loss evaluation methodology includes the following:

- classifying fraud types by evaluation principles;
- developing basic loss evaluation parameters, including evaluation periods for prevented loss;
- developing integrated indicators and principles for financial measurement of loss for each type of fraudulent activity;
- describing evaluation algorithms;
- describing a structure of reporting (operation reports, daily, monthly, quarterly and yearly reports) for internal use, decision-making and communication service provider's management.

11 Guidelines for information exchange related to fraudulent activities

These guidelines are intended for use, as appropriate, by licensed communication service providers.

It is suggested that service providers consider taking the following steps before exchanging information about fraudulent activities.

- Enter into a confidentiality agreement that defines concepts of: documentary information (document); confidential information; ownership of confidential information; information constituting a trade secret; restricted access mode; counterpart; and unauthorized disclosure of confidential information.
- Take into account the differences in legislation of the countries in question.
- Obtain a favourable opinion about its future counterpart from several proven partner telecom carriers before any cooperation commences.

In developing their cooperative arrangements with each other, telecom carriers may wish to consider:

- whether they should agree to be allowed to protect themselves, their services and clients from fraud;
- whether they should agree to be deemed equal, irrespective of differences in their status in the telecommunications market;
- whether they should agree to exchange information on instances of third party fraudulent behaviour to mutual advantage and on the basis of their confidentiality agreement;
- whether they should agree to put effort into revealing new instances of fraudulent behaviour on telecommunication networks;
- whether they should agree to enhance cooperation in revealing facts of fraudulent behaviour within as well as outside the telecommunication industry. This purpose may be achieved by encouraging closer connection between employees of information security departments and creating incentives for their further professional development;
- whether they should agree to disclose the mechanisms of fraudulent behaviour by clients, counterparts or foreign persons in accordance with the confidentiality contracts;
- whether they should strive to increase their own competence in safety issues, to make additional demands in favour of telecommunications standards, and to increase participation in research in the field of revenue assurance in telecommunications;
- whether they should coordinate their efforts against fraudulent behaviour to the mutual benefit of all telecom operators;
- whether they should provide training opportunities for experts in fraud prevention in order to raise their professionalism;
- whether they should interact through their employees who are directly responsible for detection, suppression of activity and legal pursuit of offenders.

Bibliography

[b-ETSI TR 102 647] ETSI TR 102 647 (2006), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Management; Operation Support System Standards Overview and Gap Analysis*.

[b-ETSI TS 188 001] ETSI TS 188 001 (2006), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN management; Operations Support Systems Architecture*.

[b-ETSI TR 188 004] ETSI TR 188 004 (2005), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Management; OSS vision*.

[b-ISO/IEC TR 10032] ISO/IEC TR 10032:2003, *Information technology – Reference Model of Data Management.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013