Fraud Analysis in IP and Next-Generation Networks

Definition

Fraud management systems (FMSs) are designed to detect, manage, and assist in the investigation of fraudulent events.
They rely on data provided by various elements to identify abnormalities in traffic patterns and report suspicious activity that might suggest fraudulent, irregular, or otherwise abusive activity is being engaged.

Overview

This tutorial discusses the crucial role played by FMSs in the containment of next-generation fraud, the vulnerability of Internet protocol (IP)–based technologies, effective data analysis and algorithms, and solution methodologies. The open and distributed nature of convergent and next-generation network (NGN) architecture enables easy access to services, information, and resources, together with the constant abuse of hackers, curious individuals, fraudsters, and organized crime units. Fraud perpetrators introduce new, complex techniques of fraud daily, possessing the knowledge to circumvent all network security mechanisms. Their intrusion is nearly impossible to detect, causing immense damage to operators and service providers alike.
Consequently, a new approach to fraud management is being introduced to tackle these threats.

Topics

1. Introduction to Telecom Fraud
2. IT Security vs. SP Network Security
3. IP and NGN Vulnerabilities
4. Fraud-Assisting Business Drives
5. IP and NGN Challenges

1. Introduction to Telecom Fraud

Telecommunications fraud is a multibillion-dollar business. Global estimates of direct damages resulting from fraud vary from $30 billion to more than $40 billion in 2000, or in other words, an annual loss of 3 percent to 8 percent to the average service provider. NGNs prove to be fertile ground for technological fraud and criminal activity. Recent scams of a highly sophisticated technological nature are believed to be associated with units of organized crime, cleverly employing self-educated fraud techniques and the assistance of hacking specialists. It has been said that telecommunications fraud is more attractive than the drug market. This is not to say that small-scale fraud is not practiced by millions of "everyday users" around the world. The availability of hacking information and the ease with which several illegal actions can be performed allows even amateurs to invade and abuse a network, resource, or customer account. These will more often than not result in severe loss of profit, network downtime, and/or service malfunction, subsequently creating an image of a nonsecure and inefficient network.

In NGNs, service provider losses could become considerably higher with the addition of multiple new services and increased numbers of business transactions carried out over an open, distributed network. The landscape of NGNs is a dynamic one, changing constantly to accommodate the entry of new players, mergers, and acquisitions; the introduction of fast evolving technologies; methods of access; and new billing schemes. Next-generation fraud techniques are more complex and diversified than those employed today, requiring new tools and methodologies for an effective solution. Modern day hackers and cyber criminals are often more technologically advanced than network personnel, possessing the knowledge required to circumvent existing security mechanisms far before network employees have received relevant training. Internet relay chat (IRC) enables them to exchange ideas, tips, and Web site locations of hacking tools over an open network connection, providing a wealth of dangerous information to external sources. Previous command line–based hacking has been replaced by friendly graphical user interfaces (GUIs), enabling an entire public of nonprofessionals to understand bypass procedures and commit fraudulent acts.

2. IT Security vs. SP Network Security

Traditionally, illegal network intrusions are dealt with by access-control devices such as firewalls and radius and authentication servers. However, these are not useful against the many new types of fraud devised for IP–based NGNs. The purpose for which these devices were built is highly specific and noninclusive of IP fraud possibilities; each is designed to support a single protocol (typically IP), limited to a single location, and secures only one part of the network. A firewall provides preliminary filtering of unauthorized traffic to specific resources or network segments, and a typical firewall classifies traffic on the basis of IP addresses, which are by nature unreliable. Authentication and authorization mechanisms (AAA servers, radius) restrict access to the network and its resources, enabling usage only when provided with a legal user identification and password. However, user identifications and passwords are easily obtained or guessed and therefore a user connecting to a network or service is not necessarily who he claims to be. Network intrusion detection systems (N–IDS) limit attacks on specific protocols by intercepting malicious packets and streams to particular hosts; and host-based intrusion detection systems (H–IDS) limit application-targeted attacks by intercepting malicious activity at the operating system and application levels. However, both address IT—not network—security and will not recognize fraud techniques and patterns that affect network operators.

As IP fraud may be performed from multiple points in the network simultaneously, or alternately between several different but recurring points, the successful detection of fraudulent activity requires constant exchange of information between all network elements, devices, and interfaces, followed by the comparison and analysis of all data traffic flowing through the network. Existing network elements and security mechanisms lack the ability to communicate valuable information between them, requiring the intervention of an intelligent "liaison" to monitor all interconnection points and collect, process, and distribute relevant data and ensure that all possibilities of intrusion have been covered.

3. IP and NGN Vulnerabilities

The infrastructure of next-generation/IP networks is packet based and multilayered, with open, distributed architecture and no ingrained security mechanisms. *Mission-critical applications,* used for the transmission of high-profit services such as voice, e-commerce, and financial transactions, are run over these exposed networks. With user identification based on the IP layer and the IP layer easily tampered with, packets sent over these networks can easily be marked with a 'borrowed' IP address, enabling unauthorized users to impersonate legitimate ones. These intruders abuse services and benefits at the expense of legitimate users, who are often completely unsuspecting until the bill arrives—long after the abuser has departed. This type of fraud is commonly

referred to as *IP spoofing*. The possibility that an IP address may have been altered causes data issued by the IP layer to become both insufficient and unreliable.

As said, firewalls also employ IP addresses to classify traffic and therefore cannot be viewed as an ultimate means of network security. Popular operation systems with known vulnerabilities, such as Linux, Windows, and Unix, are run on critical servers (including firewalls, radius, and authentications servers). In addition, protocols such as routing, voice-over–IP (VoIP) signaling, domain name service (DNS) resolution and e-mail (POP, SMTP) are common knowledge, enabling illegal manipulation of their transmission.

Shared mediums of communication such as cable modems, wireless transmission, local multipoint distribution system (LMDS), and others enable several indiscretions, including violation of privacy caused by eavesdropping and/or unlawful access to another user's service; password sniffing (the illegal obtainment of user passwords to be used in various scams); clip-on fraud, requiring use of a simple, inexpensive connection device that enables "free" usage of calls and a large variety of services at the expense of the operator; illegal connection to the Internet through use of an authorized user's account or ID; and impersonation of authorized, subscribing users to access the services allotted to them.

An inherent lack of embedded control mechanisms in the network infrastructure, IP– and Web-based applications contributes to low network survivability. Lack of traffic management control mechanisms enables "bandwidth theft," i.e., one user will transmit a larger amount of traffic than allocated to him, leaving other users with less bandwidth for their own use. Unmanaged congestion and lack of overload control enable sabotage in the form of denial-of-service attacks on various services (most notoriously performed on popular Web sites). One way to do this is to flood the server with repeated, legal service requests in an attempt to overload it, causing severe degradation or complete unavailability of the service to legitimate, paying users.

New billing schemes are being introduced based on content and quality, creating yet another point of weakness for criminal abuse. The better the service, the higher the profit—not to mention the availability of the scheme procedures themselves; such potential inevitably accelerates the creation of new and sophisticated fraud methodologies.

4. Fraud-Assisting Business Drives

Low customer loyalty in a highly competitive market environment demands service providers to constantly diversify their service portfolios by dynamically adding new services, upgrading service levels and increasing service flexibility.

An unprotected network subjected to recurring attacks will inevitably suffer violation of these services. It will also be exposed to the risk of customer churn due to unavailable services and network downtime. The realization that strangers have invaded and abused services and accounts belonging to paying subscribers, combined with public knowledge that severe security breaches were discovered only after subscribers had received their bill and found many unexplained transactions, contribute to bad public image and an ongoing failure to attract customers.

Customer requirements for the latest devices, mechanisms, and applications—widely purchased in order to enable effective competition and vendor business considerations, arising from the attempt to release their products within time-to-market constraints—result in a situation where many technologies are deployed before they have fully matured. As such, many products do not guarantee a secured operation, nor can they assure protection of network resources in any way.

Many fraudulent incidents remain unreported because most operators and service providers prefer to maintain a low profile when it comes to deficient network security. This could bring bad publicity, intimidate investors and other collaborators, or incite subscriber demands for a better, more secure service—entailing costly adaptation and re-enforcement of existing security measures in an effort to regain satisfaction and trust. As result, methods of attack used on one network may not be brought to the attention of all operators and service providers; enabling the same method to be used several times before it is collectively recognized and dealt with through reconfiguration of security devices. Certain fraudulent incidents involving unauthorized access to subscriber details and privileges may result in legal prosecution and liability for damages—once again at the expense of good business, revenue, and public image.

5. IP and NGN Challenges

The successful containment of next-generation fraud presents many challenges. Preliminary identification and categorization of these challenges is crucial to the implementation of a fail-safe and all-encompassing defense perimeter to guarantee maximum network security. The following list is presented to simplify the reader's understanding of security requirements in both converging and next-generation networks.

NGN Technologies

- Are open and distributed by nature
- Lack inherent security mechanisms

- Run mission-critical applications
- Become increasingly complicated
- Are deployed before they have fully matured
- Offer few expert solutions for their effective management
- Require time- and cost-consuming integration and configuration

Next-Generation Fraud

- Can be easily concealed by hackers
- Makes security mechanisms extremely difficult to maintain, as result of the following:
  - Inadequate passwords
  - Incorrect configuration of firewalls
  - Low employee awareness of security risks
  - Insufficient knowledge of NGN environments
  - Shortage in next-generation fraud specialists
- Enables fraud to be committed from multiple points in the network simultaneously
- Becomes easier to perform the following:
  - IRC channels enable free transfer of sensitive information over open connections
  - Tools, scripts, and detailed hacking instructions are publicly available on the Internet
- "Always-on" access technologies put domestic users at higher risk

Increased Incentive

- Profits from nonvoice services are rising.
- Total revenues are increasing.
- Revenues are shifting toward IP networks.

- Service value is based on content, not connection.
- Unlawful intrusion, resource abuse, and deliberate sabotage are easily committed.
- User identification, passwords, credit cards details, and codes are readily available.
- Potential for illegal gain is much higher than that offered by most first-grade felonies.

Growing Operator and SP Concerns

- Subscription fraud is increasing.
- Internal fraud is becoming a major problem.
- Hacking is no longer motivated by challenge or thrill.
- Newly devised billing schemes are being easily and unlawfully manipulated.
- New and highly sophisticated methods of fraud are introduced daily.
- Fraud scenarios are ever-changing.
- Discovery of new methods remains a "secret," enabling recurrence in another network.
- Privacy and data protection laws enable fraudsters to continue their activities.
- Most security mechanisms are only good for enforcing local access policies.

Requirements for Successful Containment of Fraud

- Security mechanisms must be complemented by a central fraud management system.
- The fraud analysis system should do the following:
  - Maintain the integrity of the entire security infrastructure

- Act against the adversary and not against the specific attempt
- Enable easy, correct configuration
- Support swift, cost-effective integration of new technologies, products, and services
- Be equipped with an intelligent means of data collection
- Detect and present results on-line, enabling immediate counteraction before severe harm is done
- Assimilate the now familiar pattern to prevent its recurrence

6. Data Collection

Data collection is the first stage in implementing an FMS. Obtaining rich, diverse information from multiple layers is a key factor for the success of an FMS in the IP and next-generation networks environment.

Various probes, IP mediation, and billing mediation products can assist in the collection of this information.

Application-Level Usage Records

Application-level usage records describe the service provided to the customer. Typically, these records will also be used for billing, since they provide all the necessary details in regard to the service used.

These billing records are typically collected from the servers providing the specific service, such as telephony services, video services, and so on.

Application-level records may be provided by the following:

- VoIP: media gateway controllers (MGCP, H.248), gatekeepers (H.323)
- Broadcast servers: music on demand, video servers
- Voice switches
- E-mail servers, Web/WAP servers

Login and Authentication Level

A typical NGN includes various login, authentication, authorization, and security mechanisms. These mechanisms are referred to as "login and authentication layer" and may provide vital information to a fraud analysis system.

Information provided by the login and authentication may be provided by the following elements:

- Radius and LDAP servers
- remote access server (RAS)
- DHCP servers
- DNS servers
- Firewalls
- virtual private network (VPN) gateways

Network-Level Information

Network-level information describes the traffic and the flows at the IP layer. This layer typically characterizes bandwidth and resource consumption.

Network elements that provide this information include the following:

- Routers and switches
- Cisco Netflow
- SNMP/RMON I + II
- Address translation (NAT)

Access Level

Access networks are used as the technology that connects the customer for the "last mile." Common technologies include cables, wireless, DSL, and dialup.

This layer holds the information about the user location. It is also aware of the hardware and Layer-2 addresses of the user terminal, such as IMSI, serial numbers, MAC address, and more.

Statistics collected by the access network are typically not affected when circumventing with the IP layer and therefore prove to be very useful for detecting irregular events.

Access-level information may be collected from the following elements:

- RAS
- CMTS
- DSLM
- Integrated multiservice access platform (IMAP)
- LMDS/WLL base stations

Triggered Content Events

Triggered content events are generated by probes, which inspect the payload carried over the network. These probes can search for text of known "exploit" scripts (used for hacking).

Triggered content events are being used today for intrusion detection systems but can also be useful for detecting elusive fraud scams.

7. Analysis Algorithms

Several algorithms were developed to detect fraud in telephony and cellular networks, much like the ones used by N–IDS and H–IDS. Universities worldwide are currently researching new IDS algorithms, with current detection methods already taking advantage of algorithms in the field of expert systems, data mining, artificial intelligence, and machine learning.

NGN and IP FMS must expand existing detection methods through the introduction of new algorithms in order to ensure detection not only of current fraud techniques but also of new and emerging ones.

Threshold-Based Analysis

Identification of fraudulent usage by means of comparing traffic patterns against predefined thresholds is a simple yet extremely effective approach. The system is based on the concept by which most losses to service providers are caused by fraudsters engaging in large-scale commercial fraud. Such a method can produce an alert, for example, the moment the number of calls being made from a certain

location exceeds the threshold of calls defined for that location. This method can be used to successfully recognize and contain theft of long, short, and/or expensive calls.

The straightforward nature of this algorithm allows simple, efficient implementation, thus allowing support of the large amount of traffic carried over telco networks.

It does, however, require fine-tuning in respect of the actual setting of thresholds, as the latter must be performed meticulously for each customer and point of contact. Moreover, this technique does not detect several types of fraud.

Inference Rules Analysis

Inference rules analysis is a fraud-containment method based on expert systems and rule production engines. It enables the preconfiguration of specific, sophisticated inference rules to determine the possible fraud types. For instance, the system administrator may feed the system the following inference rule, useful for detecting various callback scams:

>>If the caller is (*domestic*) number C

>>and the call destination is (*overseas*) number X

>>and the call length is less than 10 seconds

>>and (*overseas*) number X calls (*domestic*) number C within 30 seconds,

>>then alert on possible callback fraud; process for further investigation

Inference rule analysis can very difficult to manage because the proper configuration of such rules requires precise, laborious, and time-consuming programming for each imaginable fraud possibility. The dynamic appearance of multiple new fraud types demands that these rules be constantly adapted to include existing, emerging, and future fraud options.

Moreover, it also presents a major obstacle to scalability. The more data the system must process, the more drastic is the performance downfall.

On the other hand, these systems are very powerful and allow the detection of practically any scam or traffic pattern.

Profile-Based Analysis

Profile-based analysis can also be used to detect fraudulent activity. A customer profile is sketched according the habitual usage patterns of each user, and any

deviation from the profile is immediately brought to the operator's attention. For example, customer "Jones" is known to make a weekly total of: 5–15 local calls, 2–10 interstate calls, and 0–4 long-distance calls. The system will officiate dynamic comparison and analysis of the weekly usage records of customer "Jones" and display the relevant results.

To illustrate this type of analysis, let's inspect the VoIP calls made by customer "Jones" during a typical week (see *Table 1*):

Table 1. Jones's VoIP Calls

Name:	Mr. Jones
Customer ID:	#0667-33
Service:	VoIP

Number	Location	Duration (min.)
552-4625	NY	1.23
237-2671	TX	5.02
346-2899	NY	2.35
211-2328	CO	4.12
921-5032	MI	2.53
517-8321	NY	9.44
573-1129	NY	1.23
312-4002	NY	7.08
627-5384	GA	4.20
44-20-3441-2755	London UK	10.00
312-4002	NY	3.27
237-2671	TX	6.36
44-20-3441-2633	London UK	11.45
573-1129	NY	4.31
544-2829	NY	2.33
552-4625	NY	6.17

An abnormal call log would indicate fraud at first glance (see *Table 2*):

Table 2. Abnormal Call Log

Name:	Mr. Jones				
Customer ID:	#0667-33				
Service:	VoIP				
Number	**Location**	**Duration(min.)**	**Number**	**Location**	**Duration(min.)**
234-1-442-3611	Nigeria	125.03	234-1-442-3611	Nigeria	125.03
234-1-442-3611	Nigeria	51.34	234-1-442-3611	Nigeria	94.22
234-1-442-3611	Nigeria	45.22	234-1-442-3611	Nigeria	132.45
234-1-442-3611	Nigeria	143.54	234-1-442-3611	Nigeria	174.12
234-1-442-3611	Nigeria	156.26	258-1-702-4391	Mozambique	64.53
517-8321	NY	6.03	258-1-702-4391	Mozambique	132.44
509-237-1062	Haiti	81.43	517-8321	NY	1.23
509-237-1062	Haiti	128.27	258-1-702-4391	Mozambique	156.08
234-1-442-3611	Nigeria	110.41	258-1-702-4391	Mozambique	123.20
509-237-1062	Haiti	73.46	258-1-702-4391	Mozambique	130.00
509-237-1062	Haiti	147.04	509-237-1062	Haiti	53.27
237-2671	TX	4.35	509-237-1062	Haiti	121.36
44-20-3441-2633	London UK	10.52	509-237-1062	Haiti	104.45
258-1-702-4391	Mozambique	172.55	517-8321	NY	4.31
258-1-702-4391	Mozambique	180.43	517-8321	NY	2.33
258-1-702-4391	Mozambique	97.38	627-5384	GA	5.21

Profile-based analysis has many advantages. In addition to the clarity and ease in which results are presented, systematic investigation assists in the immediate discovery of fraud methods that were never considered, or even imagined, before the FMS revealed them. It also makes the preconfiguration of fraud rules unnecessary. However, the fair possibility the customer "Jones" has indeed established recent connections in Nigeria, Haiti, and Mozambique may result in a large amount of "false-positive" alarms, or in other words, the system may enforce security measures for what seems to be fraudulent usage of customer

"Jones" account, only to discover that said usage was perfectly legal. In addition, thorough examination of "x-positive" alarms to determine whether they are "false-positive"or "true-positive" demands long hours of laborious investigation from many employees.

Neural Networks

Neural Networks is a rather innovative approach designed to function like the human brain. The creation of this technology stems from an idea that a system simulating neural response, such as the independent assimilation of real-time data and subsequent triggering of command chains in response to this data, is better equipped to deal with machine learning than other "unintelligent" applications. Neural Networks can actually calculate user profiles in an independent manner, thus adapting more elegantly to the behavior of the various users. Neural Networks are claimed to substantially reduce operation costs. This system has one drawback: upon identifying a profile deviation, it cannot logically explain the results of its calculation—reasons for triggering the event. Moreover, the advantages and disadvantages of the profile-based analysis in the large part can also be applied for Neural Networks.

Self-Test

1. Losses due to telecom fraud worldwide are estimated around _____.
    a. $10 million annually
    b. $100 million annually
    c. $1 billion annually
    d. $40 billion annually
2. Firewalls analyze traffic _____.
    a. at the IP layer
    b. at the application layer
    c. at the physical layer
    d. at all layers
3. IP networks are less susceptible to fraud than telephony networks since they incorporate various encryption mechanisms.

a. true

b. false

4. Shared mediums allow for easier password sniffing.

    a. true

    b. false

5. Privacy laws and data protection legislation _____.

    a. allow service providers to easily prosecute fraudsters

    b. are handling only IT security issues and not network security issues

    c. may sometimes allow a fraudster to continue their scams with a different provider

    d. have nothing to do with telecom fraud

6. User location and MAC address information are typically available from _____.

    a. the billing records

    b. access network elements

    c. core routers and switches

    d. RADIUS and other authentication servers

7. Which of the following is an advantage of threshold-based analysis?

    a. It doesn't require any user configuration.

    b. It practically detects many of the fraud organizations.

    c. It is especially useful for detecting fake cellular handles.

8. Which of the following is an advantage of profile-based analysis?

    a. It doesn't require any user configuration.

    b. It is the simplest method to implement in an FMS.

    c. It is very useful for monitoring new subscribers.

9. Expert systems scale better than profile-based systems.

    a. true

    b. false

10. Which of the following algorithms has the quality that it requires minimal configuration?

    a. threshold-based analysis

    b. inference rules analysis

    c. neural networks

Correct Answers

1. Losses due to telecom fraud worldwide are estimated around _____.

    a. $10 million annually

    b. $100 million annually

    c. $1 billion annually

    d. $40 billion annually

    See Topic 1.

2. Firewalls analyze traffic _____.

    a. at the IP layer

    b. at the application layer

    c. at the physical layer

    d. at all layers

    See Topic 2.

3. IP networks are less susceptible to fraud than telephony networks since they incorporate various encryption mechanisms.

    a. true

b. false

See Topic 3.

4. Shared mediums allow for easier password sniffing.

   a. true

   b. false

   See Topic 3.

5. Privacy laws and data protection legislation _____.

   a. allow service providers to easily prosecute fraudsters

   b. are handling only IT security issues and not network security issues

   c. may sometimes allow a fraudster to continue their scams with a different provider

   d. have nothing to do with telecom fraud

   See Topic 4.

6. User location and MAC address information are typically available from _____.

   a. the billing records

   b. access network elements

   c. core routers and switches

   d. RADIUS and other authentication servers

   See Topic 6.

7. Which of the following is an advantage of threshold-based analysis?

   a. It doesn't require any user configuration.

   b. It practically detects many of the fraud organizations.

   c. It is especially useful for detecting fake cellular handles.

   See Topic 7.

8. Which of the following is an advantage of profile-based analysis?

    a. It doesn't require any user configuration.

    b. It is the simplest method to implement in an FMS.

    c. It is very useful for monitoring new subscribers.

    See Topic 7.

9. Expert systems scale better than profile-based systems.

    a. true

    b. false

    See Topic 7.

10. Which of the following algorithms has the quality that it requires minimal configuration?

    a. threshold-based analysis

    b. inference rules analysis

    c. neural networks

    See Topic 7.

Glossary

AAA
authorization, authentication, and accounting

DNS
domain name service

FMS
fraud management system

GUI
graphical user interface

H–IDS
host intrusion system

IP
Internet protocol

IRC
Internet relay chat

LMDS
local multipoint distribution system

NGN
next-generation networks

N–IDS
network intrusion detection system

POP
post office protocol

RADIUS
remote authentication dial-in user service

SMTP
simple mail transfer protocol

SP
service provider

VoIP
voice over IP

VPN
virtual private network