A view into the concealed world of telecommunication fraud

Autor(en): **Grundschober, Stephane / Schmidt, Manfred / Straumann, Hugo**

Objekttyp: **Article**

Zeitschrift: **Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology**

Band (Jahr): **79 (2001)**

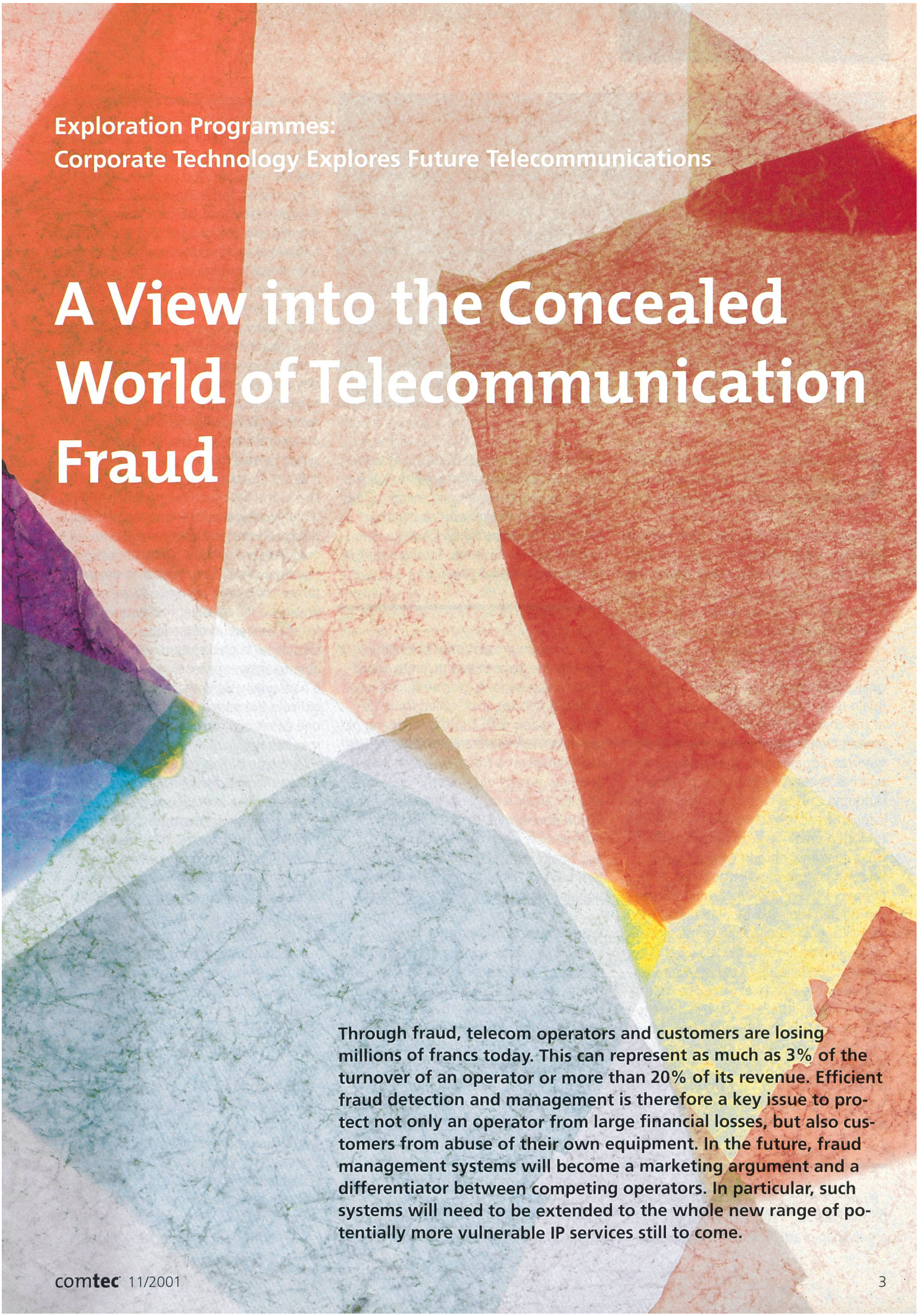
Heft 11

PDF erstellt am: **11.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-876588

Exploration Programmes:
Corporate Technology Explores Future Telecommunications

A View into the Concealed World of Telecommunication Fraud



Through fraud, telecom operators and customers are losing millions of francs today. This can represent as much as 3% of the turnover of an operator or more than 20% of its revenue. Efficient fraud detection and management is therefore a key issue to protect not only an operator from large financial losses, but also customers from abuse of their own equipment. In the future, fraud management systems will become a marketing argument and a differentiator between competing operators. In particular, such systems will need to be extended to the whole new range of potentially more vulnerable IP services still to come.

The Exploration Programme "IP Business Support Issues" deals with technologies, services and support functions for IP networks. In detail these are:
- Content oriented IP billing; technologies needed to charge for IP services.
- MPLS Traffic Engineering; how to enable the support of IP-VPN point-to-cloud SLAs with end-to-end QoS guarantees.
- Fraud; what kind of fraud is to be expected when offering services on IP networks and how to prevent such fraud.
- Mobile devices security; which privacy services can be offered for GPRS and UMTS devices accessible from the Internet.
- Security services for the massmarket; easy-to-use security services for Internet users.

With its Exploration Programmes, Corporate Technology is exploring telecommunication technologies and new service possibilities with a long-term view of 2–5 years. Furthermore, the expertise built up in the course of this activity enables active support of business innovation projects.

STEPHANE GRUNDSCHOBER,
MANFRED SCHMIDT AND
HUGO STRAUMANN

Fraud Detection for Voice over IP

Criminals do often seem to dispose of amazing resources when it comes to finding weaknesses in systems. Indeed, among the many known fraud methods, one is particularly popular within fraudster circles. It is the PBX (Private Branch Exchange) fraud. The goal is to take over an enterprise PBX (plain telephony), in order to place calls at the charge of the PBX owner. This is made possible by using various system features. For example, the voicemail system is sometimes configured to allow outgoing calls to be placed after one has listened to all messages. This can be useful for an employee working at home to call a customer abroad without going through complex and error prone expenses recovery. But what an employee can do, a hacker will be able to do, too. He will spend quite a time trying all kind of passwords, until he finds a valid one. He will then be able to place calls to foreign countries for free: after one month worth of calls, the bill is charged to the PBX owner. For a small enterprise this can even lead to bankruptcy when the bill jumps to 100 times the normal amount, and in any case causes credit recovery difficulties for the operator, if not plain losses.

"Piraterie: coups de fil à l'œil" (Hacking: phone calls for free). This was the title of a newspaper article in the "Tribune de Genève" on January 13, 2001. The article described the efforts of the police investigating the scam and trying to find the criminals. Similar articles could be found at the same time in Austria, Italy, and throughout Europe. Total amount of losses: more than 9 Mio Euro.

How to counter such attacks? Within fraud management and revenue assurance organisations, we can find a very effective fighting tool, called fraud detection system (FDS). In the following paragraphs we will describe the goal and key features of a fraud detection system and how it can help both the operator and its customers. We will then look into future developments, the possibility of marketing a fraud detection product, and finally what a fraud detection system will look like in an IP environment populated with new services.

Fraud Detection Systems

In an ideal world, there would be no security or fraud problems, as the equipment would be absolutely safe, the people would be attentive to security issues, and the criminals would leave enough traces to get caught. But reality is far from ideal. Actual systems are so complex that even the best intentioned administrator will inevitably leave weaknesses in the configuration – and we are not even talk-ing here about unavoidable, non-technical risks. Criminal fraudsters will amazingly find such weaknesses and exploit them in order to gain money. The consequence is that although you spend a lot of time configuring and securing your systems and processes, you still need to put in place a damage limitation system limiting the losses to a minimum when an intruder exploits your system.

A fraud detection system could be called the fire detector of telecommunication: it rapidly detects any suspicious behaviour and allows a rapid reaction to the discovered threat through an ad hoc process, limiting the losses to an acceptable minimum. The necessary fast reaction time is achieved by analysing in real-time all communication information generated by the network, i.e. calling number, called number, date and time of day, and duration, by extracting it directly from the signalling network (SS7). With this basic information, combined with historical data, the system is able to distinguish between normal and fraudulent phone usage. Figure 1 shows the basic architecture of an FDS [1], a highly integrated system ranging from data collection to alarm presentation via complex data analysis, and with a strong real-time orientation. Note that simple database tools from billing or data warehouse would not meet the requirements for efficient fraud detection.

Of course, such a system will never be able to answer precisely whether or not a particular user is a fraudster. It will only indicate the possibility of fraud by using one of various methods to judge customer behaviour:
- One type of analysis is based on previous knowledge of basic customer behaviour (like average bill per day/week/month, proportion of international calls, typical time of day of calls, etc.) and known pattern related to fraud (international calls to hot destinations, number of different called numbers, long duration calls, etc.). This apriori knowledge is coded into sets of rules that are used by the system to evaluate an account. If the calls made with this account exceeds a rule (for example a maximum bill amount), the rule is triggered. The more rules triggered, the more suspicious the account.
- The second type of analysis involves more "intelligent" techniques. They are often trying to identify a shift in a specific customer call pattern. For example, the identification of an exponential international traffic pattern for an enterprise would lead to the suspicion of a PBX hacking. These techniques use diverse fuzzy algo-

rithms, neural networks, clustering, etc. [2]

Detection is an important aspect, but reaction is the goal. Indeed, it does not help to detect suspicious activity within 10 minutes if it then takes 6 hours for a reaction to happen. In fact, a team available 24 hours a day is required, as fraudsters are mostly active at night or during weekends. The process must be clearly defined: How are cases prioritised, who decides if and what kind of immediate actions should be taken, who takes contact with the suspicious customer... The analysts need to understand exactly who the customer is they are analysing: could he really be a fraudster, or is he just a good customer using many different services, legitimately purchased? The frontier between the two cases is often blurred and asks for most sensitive analysts.

New Challenges: IP Everywhere

It is worth noting that the current fraud issues refer to a technology – plain telephony – that is technically mature and running for decades on Swisscom's own equipment. With the advent of the Internet as a universal communication platform this is about to change. The possibility to create new complex telecommunication services with ease, relying on the skill of millions of webdesigners and programmers world-wide, has already changed the telecommunication industry: the available bandwidth has increased dramatically and is waiting for exploitation, and new players enter the telecommunication area (e.g., Microsoft's .NET initiative [3]). To be able to utilise this bandwidth, telecommunication operators are going to offer

- broadband content (e.g., movies, software, etc.),
- services that are adding value to the customer (directories online, single-login, unified messaging, etc.),
- device-independent access to content and services,
- integrated solutions through co-operation with third parties.

This will bring about new risks and possible pitfalls – beside the current ones that will inevitably remain. To name a few:

- Who is responsible if valuable content is redistributed? In these new services, the value of the content may exceed the value of the transmission by far.
- How is the customer/transaction information shared among partners? A complex integrated solution – like e-banking via a GPRS enabled mobile phone – involves many different partners, who need various information diversely classified and protected. In such an environment, is an operator alone still able to detect fraud with the data available?
- There is a strong business pressure to roll-out new services quickly, although such complex applications are asking for high security and thorough testing.

Moreover, fraud detection in the emerging era of "IP everywhere" will become even more difficult due to privacy issues: With customers migrating more areas of their private life to the "net" (buying food, holiday trips, managing his bank account and shares, watching movies, ...) and accessing services via multiple devices (PC, Mobile, PDA, etc.) a fraud detection system will need to combine all available information so that the customer himself will be subject to investigation. If we go on like today trying to analyse customer behaviour to detect potential fraudsters, the issue of respecting customers privacy is thus going to emerge [4].

To address the challenges of future fraud, we have to come up with different approaches, suitable for the 21st century:

- Make the *trust model* explicit: how far can an operator trust customer XY? Is he/her allowed to make unlimited phone calls to an unlimited number of international destinations?
- Be sure to address *risk management* in the service development process: how will we know that we are defrauded? How to minimise the risks and costs associated with it?
- *Strong encryption* is already now being used to protect access and content ('watermarking'); this seems to be the most promising technology to protect customers and operators alike.

Conclusions

A fraud detection system is currently the best answer to the fraud threat: It is specially designed for fast analysis (near real-time) and response to traffic events on a "per customer" basis, whereas a billing system usually runs once a month, and a data warehouse produces aggregated data only.

Efficient fraud detection protects the operator against losses or debit recovery difficulties, and allows to inform customers on hacking attempts (or successes) against their equipment, or to make them aware of the running up of their bill (for example due to a misconfigured dialup router, to the excessive use of Premium Rate Services, ...). It is even possi-

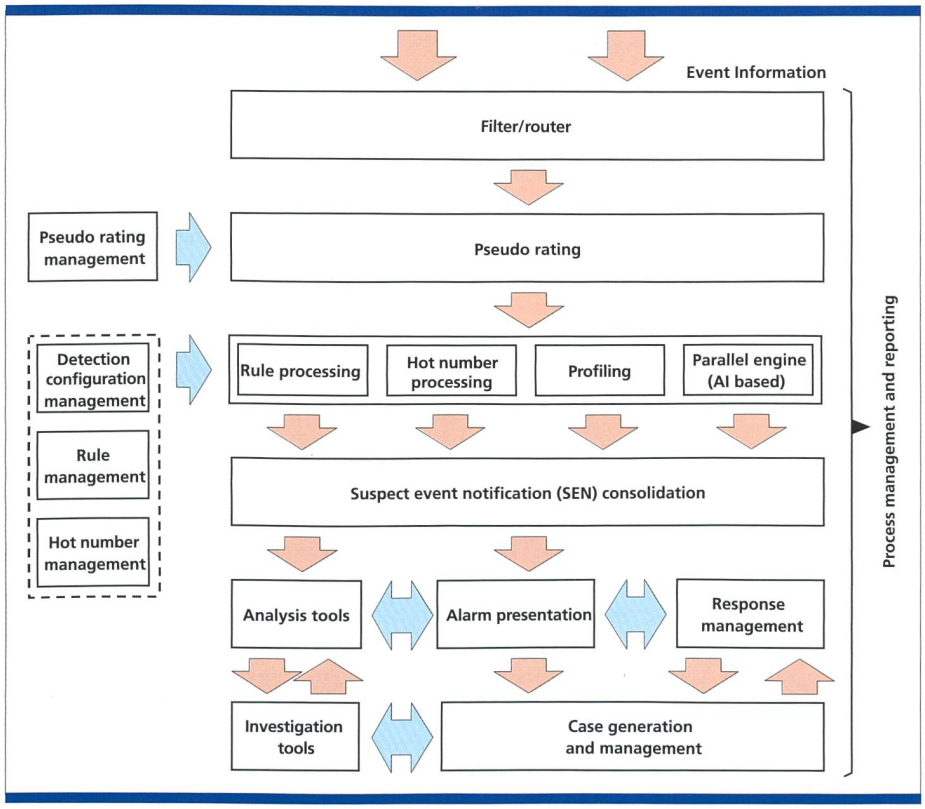


Fig. 1. Fraud detection system architecture ((c) FML [1]).

ble to actively market a fraud detection product: An operator would then agree in an SLA (Service Level Agreement) to inform a customer within a predetermined number of hours of suspicious activities, or even propose a risk transfer from the customer to the operator given certain conditions fulfilled by the customer. Insurance is here the keyword and will certainly play an increasing role in future telecommunication (and IT) service offerings. Efficient fraud detection services will be a marketing advantage over competing operators.
Another extremely important aspect is how an operator compares to other international operators in fraud prevention. Fraudsters are organised internationally, and move their operations without difficulties from one country to another. It will not take long for them to find the operator with the poorest fraud management in place, and exploit it without mercy.
As IP is becoming more important in new products, it will also modify the way we will handle fraud. Although parallels can be seen between classical fraud and IP fraud, we need to understand exactly what indicators are carrying the most evidences for fraud. The current situation is simple: minutes equal money. But in the future, a session or a content will be equal to money, and not a time interval anymore. Fraud detection systems will need to support additional information sources, including new semantic, and extract relevant information for an efficient risk assessment. Consolidation of all these sources into a coherent "account" perspective will be a challenge. Finally, the fraud analyst will need a much broader knowledge of the various products monitored and their possible interaction.
Along with the diversification of players involved in the delivery of future products, it will be more difficult to define the area of responsibility, and the processes of incident handling are going to be much more complicated, even getting into the area of data protection.
A new era of fraud detection is opening as we are stepping into the new millennium, and the problems, conceptually, are far from being resolved.

Outlook

Swisscom Corporate Technology will further explore means and measures to protect customers and services. In the near future we will take a closer look at the service creation process at Swisscom, to support the creation of sufficiently secure services for our customers.
Besides offering security support for Swisscom Group Companies, Corporate Technology will constantly look out for new technologies and new approaches to protect our future businesses. [4]

Stéphane Grundschober *studied Communications Systems at the Swiss Federal Institute of Technology (EPFL, Lausanne) and Eurecom (Sophia-Antipolis, France) from 1993 to 1998. He wrote his Diploma thesis at the IBM Research Laboratory Rüschlikon in the field of Intrusion Detection. Since 1998 he has been working at Swisscom Corporate Technology on computer security and fraud in telecommunication services.*

Manfred Schmidt *has been working for Swisscom Corporate Technology in the field of security and service management since 1999. Besides telecommunication fraud he is interested in all kinds of data analysis in telecommunications. He studied mathematics and electrical engineering in Dortmund (Germany) and received a Ph. D. from the faculty of science, University of Bern in 1999.*

Hugo Straumann *received a master of science degree at Ohio University in systems engineering. He worked in Japan as project manager and in Switzerland as head of development for access control systems and alarm detection systems. Since 1996 he has worked at Swisscom AG in various projects. His focus is: security and risk analyses in general – security management consulting – business, process and holistic risk analysis – risk analysis methods – EOQ quality systems management.*

Zusammenfassung

«Fraud» ist der Oberbegriff für verschiedene Möglichkeiten des bewusst betriebenen Missbrauchs nicht berechtigter Personen von Telekommunikationsdienstleistungen. Fraud ist weder eliminierbar noch Schicksal. Mit einem optimalen Prozess und den richtigen Erkennungsmitteln kann Fraud eingedämmt werden. Ein Fraud-Detections-System gehört heute als Erkennungsmittel zum Standard, wie auch ein Expertenteam nötig ist, um in der Sicherheit nicht hinter der Entwicklung zurückzubleiben. In Zukunft werden uns die IP-Systeme noch weit mehr fordern, um Fraudverluste in ihre Schranken zu weisen. Es ist unabdingbar, Sicherheitsaspekte in den Produkten von Anfang an mit zu berücksichtigen. Die Frauderkennung muss zudem auf neuen Indikatoren basieren. Swisscom Corporate Technology erarbeitet und unterhält das notwendige Expertenwissen über die aktuellsten Technologien, Frauderkennungsverfahren und Gefahrenlagen.

References

[1] FML, "Fraud detection system logical architecture", 2000, http://www.fmlsolutions.com

[2] Eurescom project P1007, "Application of Intelligent Techniques to Telecommunications Fraud Detection", 2nd deliverable, January 2001

[3] Microsoft, "Microsoft.NET", http://www.msdn.microsoft.com/net

[4] Swiss government, "Data protection law", 1992, http://www.edsb.ch/data/showme9547.html

Abbreviations

FDS	Fraud Detection System
GPRS	General Packet Radio Service
MPLS	Multi Protocol Label Switching
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
SLA	Service Level Agreement
SS7	Signalling System #7

Pointers

Information about telecom fraud:
http://www.agilent.com/cm/commslink/hub/issues/fraud/index.html
http://www.att.com/fraud
Fraud insurance:
http://www.lucent.com/press/0196/960130.gba.html