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

Herausgeber: Swisscom

Band: 80 (2002)

Heft: 5

Artikel: Minimising the risk for 3G

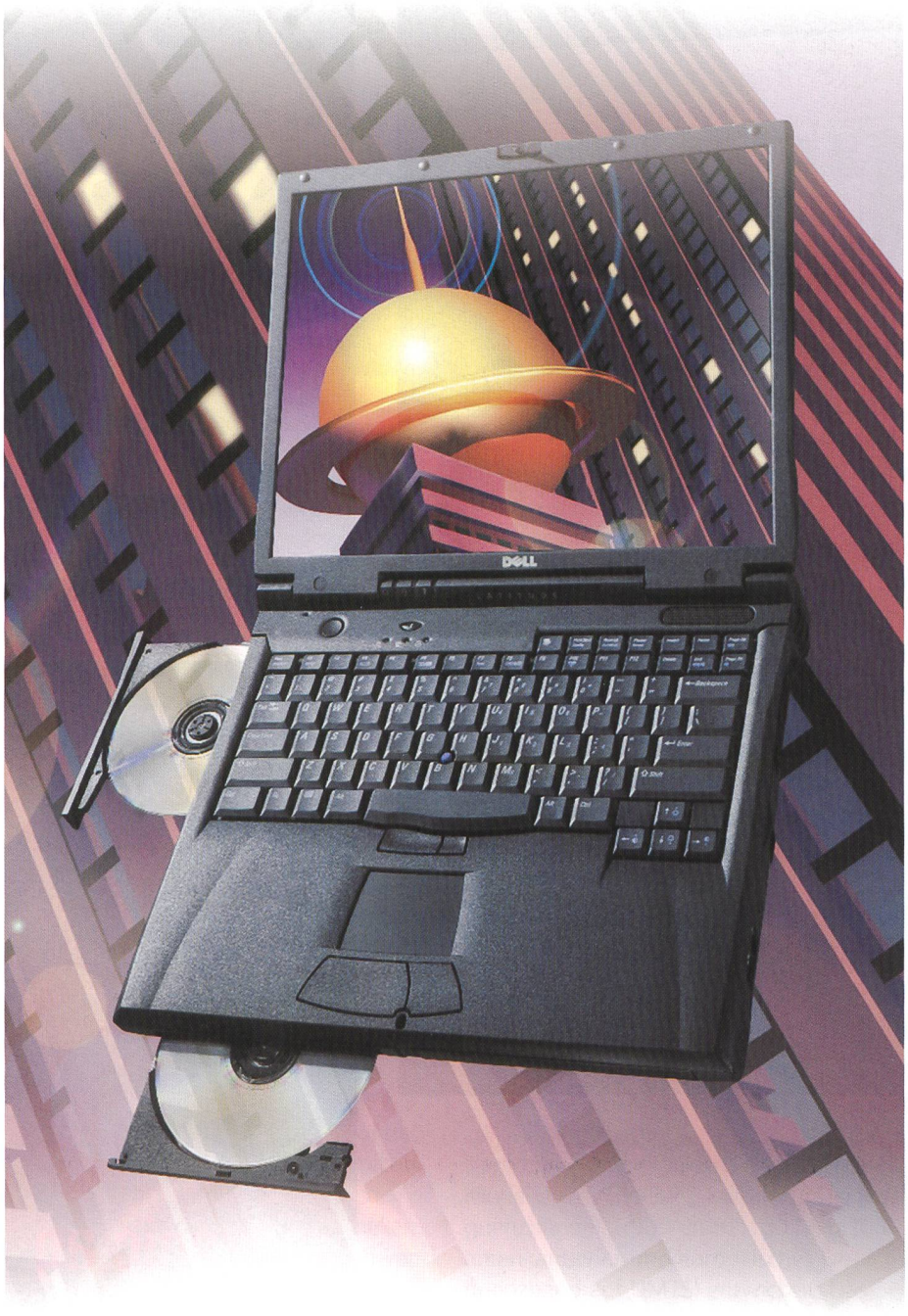
Autor: Mason, Peter

DOI: https://doi.org/10.5169/seals-877202

Mobile Fraud

Minimising the risk for 3G

Telecom fraud has become a bigger organised crime than drug trafficking. Over 750 million pounds of business is written off as "bad-debt" each year by British telecom companies, most of which is blamed on fraudulent activity. Analysts estimate that the worldwide industry loses up to 50 billion pounds worth of business to fraud each year, and the number is increasing with the growing popularity of mobile phones.



Dell

Analysts estimate that the worldwide industry loses up to 50 billion pounds worth of business to fraud each year.

PETER MASON

The launch of 3G mobile handsets in particular will bring about even greater risk for fraud, thanks to the increased complexity of data and information passing through the network. With most telecom companies already trying to cope with repayment loans for 3G licenses, the option of writing off fraud loss as bad debt seems impossible. The only way out of the financial burden is to combat mobile telecom fraud through early detection and protection.

Subscription Fraud

The most popular kind of fraud committed on mobile handsets is subscription fraud, whereby the criminal manipulates databases and user identities to receive free telecom services. 3G technology offers many opportunities for this type of fraud to occur, since it introduces a wide range of new applications and services such as web, VoIP, data, and video functionality. The personal financial risks associated with 3G handsets are also greater than with other mobile technologies, since there is more personal information on display for fraudsters to exploit – such as credit card and banking details – which are used to pay for online products and services.

Mobile phone cloning is another major problem for mobile operators. This type of fraud allows hackers to make free international and expensive roaming calls. More than 900 million roaming calls are made on GSM networks each month, helping to produce 10% of annual revenues for European operators. The main problem behind 3G roaming fraud is the delay in the communication of billing information between the operators and

the difficulty of analysing information that is encrypted or lost. According to GSM guidelines, the serving carrier is responsible for providing a home carrier with roaming call detail records (CDRs) within two days of the call being made. Within this timeframe, organised criminals have a window of opportunity for making millions of pounds worth of calls. Once this type of fraud occurs, the financial burden is carried by the user's roaming operator, who must pay the operator of the roaming network for the roaming privileges.

3G – Easy Target for Criminals

Despite its sophisticated technology, the 3G network will be even more susceptible to these popular kinds of fraud attacks. The reason for this stems from the vulnerability of its IP packet-based infrastructure. As packets of information move through the network, hackers will have the opportunity to seize some of these data units, and change, use or destroy the information. The rapid increase of IP traffic will also make it hard for 3G operators to detect unlawful use in the network. Unlike other telephone networks, 3G will not necessarily have a centralised device – like a switch – to gather network data and information. Instead, IP information will be created from numerous devices and will come in different volume sizes, enabling criminals to commit fraud across different points within and outside the network. Operators will also find it difficult to pinpoint the source of data to a particular subscriber or carrier, since packets can travel across many technical boundaries on their journey. A fraudulent attack can occur on one network and not be obvious when the data passes into other networks. This makes it tricky to assess the possibility of fraud, since operators need to analyse the content in the data packet and match it to the correct network privileges of the customer. The loss of the switch-based circuit also means that much of the traditional audit capability of fixed line and 2G networks is lost.

Emphasis on fraud systems

The complexities of the 3G network will require a fraud system that can cope with the numerous tactics of the criminal. One of the most important features that operators should look out for when choosing the right system is flexibility, since there is still uncertainty as to what types of services will be introduced by 3G, and which of these services will be attacked by hackers. Operators will require the ability to change and modify rules to address new and evolving fraud methods. Call finger printing and subscription fraud analysis will also be important to help detect more sophisticated criminals on the IP network.

Securing 3G's profitability

Finding the right fraud system will be as vital to 3G's revenue performance as the services that operators will offer. To compliment any system, fraud management providers must establish close ties with their billing, network management and inter-carrier teams to keep on top of the latest trends in fraud detection and prevention. By sharing information operators can optimise the success rate of the fraud management program help secure the profitability of 3G technology. 9.3

Peter Mason, *Revenue Assurance Manager, Intec Telecom Systems.*

Intec Telecom Systems is a global provider of OSS for fixed, mobile and IP networks. The company can be contacted by phone +44 1483 745 800 or via www.intec-telecom-systems.com
Intec Telecom Systems were an exhibitor at Billing Systems 2002, 22–25 April at Earls Court Conference & Exhibition Centre. Billing Systems 2002 – now in its 9th year, the event was firmly established as the largest and most important event in the European Billing calendar. For further details contact billing@telecoms.iir.co.uk or visit www.iir.co.uk/billing
This article has been written as part of a series of articles for Billing Systems 2002.

Zusammenfassung

3G-Betrug: Wer in die Vorbeugung investiert, spart Milliarden

Telekommunikationsbetrug ist ein Problem, das heute keinen Anbieter mehr verschont, ja, mit der Technik der nächsten Generation werden die Betrüger eine noch viel grössere Informationsmenge ausschlachten können. Die Vielzahl der neuen Anwendungen und Dienste, die 3G möglich macht, warten nur darauf, geplündert zu werden, sei es das Internet, VoIP, die Datenübertragung, die Videoübertragung oder spezielle Transaktionen. Mit der Vervielfachung der neuen Dienste könnte der Betrug ein nie für möglich gehaltenes Ausmass erreichen. Branchenanalytiker schätzen, dass dieser Betrug die Betreiber heute schon annähernd 3% ihrer Erlöse kostet und die Branche jedes Jahr über 50 Milliarden Pfund verlieren lässt. Allein in Grossbritannien beläuft sich die Einbusse auf über 500 Millionen Pfund.