Basset Telecom Report

Following the money – the **drivers** of fraud

All reports and studies on fraud in recent years show that fraud is costing operators billions of dollars yearly on a global basis. Even if the levels of loss due to fraud vary from operator to operator and from market to market, one trend is clear: Fraud and security threats increase with the expansion of the next generation IP-based networks.

Fraud is a major concern amongst operators. This paper explains the underlying market situation for fraud and the fraud threat in the next generation networks. It also provides examples of what countermeasure capabilities operators need to have in place in order to prevent and embrace a more proactive approach on fraud. Exactly what types of new fraud attempts we can expect in the next generation networks and how this expanding threat will affect carriers, operators and most importantly the subscribers is, to a large extent, left in the dark. However, there are several effective ways of addressing these issues that subscribers will take notice of and appreciate. It is an urgent matter for all operators.

Millions of malicious code signatures on the Internet and new innovative fraud methods make every next generation networks operator very worried about threats deriving from fast moving cyber criminals, now and in the future. Fraud and industry experts share the view that the opportunities of fraud will multiply with the rapid growth of gadgets, services and applications connected to mobile networks and the Internet [Ref 1]. Understanding the market challenges for fraud and revenue management and knowing how to address the most common and expanding types of fraud is crucial for securing the overall business and keeping customers safe from cyber attacks.

In order to be successful in the fight against fraud, operators need to have a strategy in place and also have a clear focus on winning the trust of their customers or subscribers [Ref 2]. Otherwise, the consequences will not only put operators at a financial risk due to more losses. It will also, if operators fail to guarantee a safe connection and usage of services or applications, endanger the subscriber business model due to growing number of dissatisfied customers, and as a consequence a very possible increase in churn rates. The good old days when churn more or less could be ignored is over. As mobile Internet services more and more becomes linked to money and financial services, like mobile money and banking functions, winning the trust of the customer becomes even more important.

INTERNET SECURITY THREAT FIGURES, 2010:
286 million – number of unique variants of malware detected.
1 million – number of zombie computers controlled by Rustock botnet.
260,000 – average number of personal identities exposed in each corporate attack.
6,253 – number of new software vulnerabilities that could be used by criminals.
42% – increase in the number of vulnerabilities on smartphones.
14 – number of never-before-seen 'zero day' vulnerabilities that first turn up in malware.
2010 Internet Security Threat Report, Symantec

WHY TOTAL CONTROL IS KEY

The unfortunate reality today regarding fraud is that many operators fail to keep pace with ongoing changes to the application and threat landscapes, particularly due to the massive growth in smartphones, the applications (apps) market [Ref 3]. Smartphone users do not only download more apps than the average regular mobile phone user. People with smartphones often use their phones more often for gaming, transactions and social networks like Facebook, which happens to be the most used web application amongst mobile users in the US, according to a Nielsen study [Ref 4]. The pattern looks the same in Europe and the rest of the world. In combination with the expected high adoption of cloud services amongst mobile Internet and smart phones users, this will put the greatest strain on the networks when it comes to fraud attempts. Today's bypass-, PBX-hacking- and International Revenue Share (IRSF) fraud methods, will tomorrow be malware, hidden in apps and web services, targeting online banking accounts, sensitive private information as well as confidential corporate information. Until now fraud attacks has mostly caused pain to businesses and organizations, but now they are causing pain to the end-users as well [Ref 5].

As we know from the IT industry, malware will not only degrade the quality of service, but also endanger the trust of the subscriber, which is enough to lose a customer.

The basis of dealing with fraud threats, both inside and outside, is control. Not only on quantity of data, but also on controlling data patterns. Simply because the more accurate data there is to analyze the more accurate analysis you get [Ref 6].

TO BE ABLE TO WIN THE BATTLE AGAINST FRAUD IN TELECOM SYSTEM IT IS NECESSARY TO DEFINE FRAUD. THIS IS BASSET'S GLOBAL DEFINITION OF FRAUD:

Fraud in telecommunications is when someone gains access to services or products that is sold through a telecommunications system and uses this information or service in a damaging or fraudulent way. Fraud also includes internal fraud and exploitation of services/loopholes through errors that have a bearing on billing, payment or provision of telecommunications services or networks.

THE IMPORTANCE OF HAVING A FRAUD POLICY

Having an effective fraud policy in place is not just an issue for the IT-department. It needs to be part of a corporate policy because the bottom line in dealing with fraud is a question of trust. To ensure a superior level of fraud prevention and detection operators need to focus on behavioural analysis of data traffic and internal security measures. Often the most destructive fraud attacks come from the inside, which is difficult to detect. Only strong leadership, training and a well-structured organisation can meet this challenge. In practice it means having the following in place [Ref 7]:

- Extensive intelligence overview of traffic streams and applications
- Access to contextual information and intelligence combining fraud and revenue assurance
- Flexible but yet detailed control and detection functions with a multi-layer threat prevention system
- Extensive analysis tools of data
- Active testing methods that reveal fraudulent activities and revenue leakage
- Internal fraud awareness programs, such as whistleblowing, vetting processes

THE IMPORTANCE OF USAGE PATTERNS

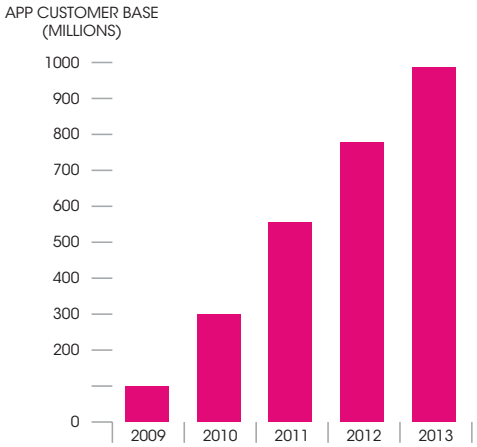
One of the most effective ways for operators working proactively to prevent fraud is to know the subscribers. Not just who they are but also be able to seamlessly and transparently see the applications and traffic patterns of each subscribers as well as aggregated data, which can be used as intelligence like for example: The security status of the endpoint device being used, the user's location, the type of network connection being used and when it is being used. Any communication session can include malware and other types of threats capable of infecting and damaging an IP-based network. The main objective of multi-layer threat prevention is to detect and find the loopholes that can be detected by behaviour anomaly-based analysis engines. The basis for this is to have specific policies so all users can be followed from one location to the next:

MOST COMMON CYBER THREATS FOR SMARTPHONES (NEXT GENERATION NETWORKS) [REF 8]:

1. Data leakage resulting from device loss or theft
2. Unintentional disclosure of data
3. Attacks on decommissioned smartphones
4. Phishing attacks
5. Spyware attacks
6. Network Spoofing Attacks
7. Surveillance attacks
8. Dialler ware attacks
9. Financial malware attacks
10. Network congestion

SEEING IS BELIEVING

Reports, data navigation utilities and analytic tools are required to help understand what is actually happening on the network, but without the visualisation it is almost impossible to get an overview of what applications are being used, by which users and to what extent. This requires real-time monitoring capabilities and activity summaries that can easily show historical data as well as specific details.



MAIN MARKET DRIVER FOR FRAUD (STATISTICS ON SMART PHONE USERS AND MOST USED APPS) [REF 9]**:**

Eliminating fraud is ultimately a question of trust and operators should also take into consideration expanding their responsibility outside their own networks and networks of their partners, whether it is through roaming or interconnect usage agreements and contracts. Indifference of threats or fraudulent behaviour can also include services or applications that are exploiting children or persons in a vulnerable position. Therefore it is also appropriate for operators to discuss the areas including the protection and safety of the subscribers and the relation between the consumer's responsibilities versus the operational responsibilities.

When evaluating methods for improving fraud prevention, operators could also take in account the possibility of protecting customers in vulnerable situations by actually blocking destructive services. Today's wide spread use of parental control tools for computers is a good parallel example of how mobile users could protect themselves from sites (or apps), which main focus is luring money from innocent visitors. Or help protecting children and teenagers against miss-use or overconsumption of quick and easy but very expensive instant loans. As the mobile world is emerging with the Internet world the demand for these possibilities will arise sooner or later. It is even possible that this type of proactive offerings or measures could lead to a more positive revenue stream for operators, since it displays a clear example of responsible customer care and goodwill. It may even pay off if you position yourself as the safe and caring operator. In the end it is all about winning the battle of the subscribers.

In conclusion:

- Fraud is driven by the strong growth in using mobile Internet
- Social networks, apps and web sites hide malware
- Criminal networks behind more advanced and disguised fraud methods
- Operators need to have a fraud policy in place and define fraud
- Necessary to use a combination of methods and analysis tools to detect and prevent fraud

REFERENCES

Ref 1 In-depth interviews with experts and clients in Basset Telecom Report

Ref 2 In-depth interviews with experts and clients in Basset Telecom Report

Ref 3 *Global Smartphone Application Market Report 2010,* research2guidance

Ref 4 *Mobile Apps Playbook September 2010,* The Nielsen Company

Ref 5 *2010 Internet Security Threat Report,* Symantec

Ref 6 *Information security technical report 13 (2008) 247–255,* Elsevier Ltd, Edward Humphreys

Ref 7 *A Market Research Report & Analysis of Telecommunications Carrier & Vendor Opportunities,* October 2006, Technology Research Institute

Ref 8 *Smartphones: Information security risks, opportunities and recommendations for users,* December 2010, ENISA

Ref 9 *Global Smartphone Application Market Report 2010,* research2guidance

GSMA

The GSMA represents the interests of mobile operators worldwide. Spanning 219 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, Internet companies, and media and entertainment organizations. The GSMA also produces industry-leading events such as the Mobile World Congress and Mobile Asia Congress.

ENISA

ENISA is the EU's response to these cyber security issues of the European Union. As such, it is the 'pace-setter' for Information Security in Europe, and a center of expertise. The objective is to make ENISA's web site the European 'hub' for exchange of information, best practices and knowledge in the field of Information Securit

BASSET TELECOM REPORTS

Basset Telecom Report is an annual series of White Papers. They provide an overall summary of the challenges operators are facing in the next generation network marketplace, and what operators need to consider and understand in order to be an effective, attractive and profitable player. The Basset Telecom Report consists of four white papers, covering the following specific areas: Roaming, Interconnect, Fraud in the next generation networks and Quantifying fraud in the next generation networks.

BASSET

Basset is a global provider of Business Support Systems for telecom operators within inter-operator billing and revenue assurance. As an advisor we are committed to help operators get more out of their business by providing solutions within inter-operator billing and revenue assurance that ensures operators get paid for every transaction in their network.

Basset serves more than 70 customers in 65 countries. Basset helps several operators growing their business and reach operational excellence in more than one domain. Among Basset's customers are Zain, Telefonica, Millicom, Globe Telecom, Etisalat, Tele2, Cable & Wireless, Vodafone, Orange and Airtel. Working with so many operators around the world has given Basset the experience that makes them the ideal partner when operators want to grow their businesses.

Basset is a part of the Kinnevik Industrial Group, which was founded in 1936, and is one of the largest listed investment companies in Europe. Please visit: www.bassetglobal.com for more information.

Phone: +46 (0)8 562 676 00
Fax: +46 (0)8 28 62 31
Löfströms Allé 6C PO Box 1156
SE-172 23 Sundbyberg Sweden
www.bassetglobal.com