Protecting Against the Next Generation of Telephony Fraud

A Telsis White Paper
December 2015

Telsis

Introduction

Telephony fraud is evolving rapidly. In the past, criminals had to trick users into performing some action that allowed the fraud to take place. As we move into the world of IP telephony new techniques are being developed by fraudsters that no longer require any user intervention. As a result, customers may not spot the fraud until a large bill from the operator drops through their door.

Customers expect their network operator to protect them from these threats. Surveys indicate that customers see fraud prevention as an increasingly important factor when making a decision about their choice of network operator.

This white paper provides an overview of telephony fraud, anticipates the threats posed by next generation fraud techniques and offers practical steps that network operators can take in order to protect their customers and their networks from these new types of threat.

A History of Telephony Fraud

Since the origination of the first telephony services, criminals have sought ways to use them for fraudulent purposes. Early types of fraud were basic (such as using the phone to impersonate someone), however fraudsters have become more sophisticated and the types of fraud being perpetrated have become far more difficult to detect and prevent.

Traditional switched telephone networks have suffered from a range of different types of attack by fraudsters. Some of the techniques used have included:

Impersonation Fraud

This is the most basic type of telephony fraud. Fraudsters simply call people pretending to be someone else. For example, they may phone a bank and ask them to transfer money from their target's bank account to another account.

Today improvements in audio quality and security checks mean that basic impersonation fraud has declined, however it is still used by those implementing phishing attacks.

Payphone Fraud

Payphone fraud was a type of fraud where users would try and get free calls from payphones.

With advances in payphone systems and their decline due to the introduction of the mobile phone, payphone fraud has generally disappeared however there are still some types of payphone fraud that take place in emerging markets.

Premium Rate Service (PRS) Fraud

Premium rate numbers are numbers that as their name suggests, are charged at a higher rate than normal person-to-person calls. Fraudsters use a variety of techniques to get unsuspecting users to call their premium rate number and have been able to make significant sums when successful.

PRS fraud has been combated by increased regulation and the introduction of different revenue models.

International Revenue Share Fraud (IRSF)

This is similar to PRS fraud, however in order to overcome regulations and delays in receiving revenue, the fraudster moves to another country with more liberal regulation. They then trick callers into calling international premium rate numbers rather than national numbers. This makes it far more difficult to police.

With mobile phones, the situation has become more serious. If a roaming subscriber has their phone stolen in one country, fraudsters may use it to make calls to a premium rate services in a third country making it difficult to trace across three territories.

Wangiri

Wangiri (literally, "One [ring] and cut") is a type of fraud that originated in Japan. The aim of Wangiri is to get users to call a premium rate number (national or international).

When the user sees the missed call on their mobile, they think that it is a genuine missed call and call the number back. They are then charged for this call. The fraudster may simply play ring tone for a period of time leading to increased call durations.

Call Forwarding Fraud

Call Forwarding Fraud uses Private Branch Exchange (PBX) call forwarding services to divert incoming calls to a premium rate or an international premium rate number. The fraudster either obtains physical access to a PBX extension, tricks a PBX user to configure call forwarding or accesses a poorly configured PBX management service to enable call forwarding. By then calling the extension which has call forwarding enabled, the call is forwarded to the premium rate number and the fraudsters receive revenue for those calls.

Call Forwarding Fraud may be eliminated by properly secured PBXs that do not allow calls to be made to premium rate or international numbers.

Call Clearing Fraud

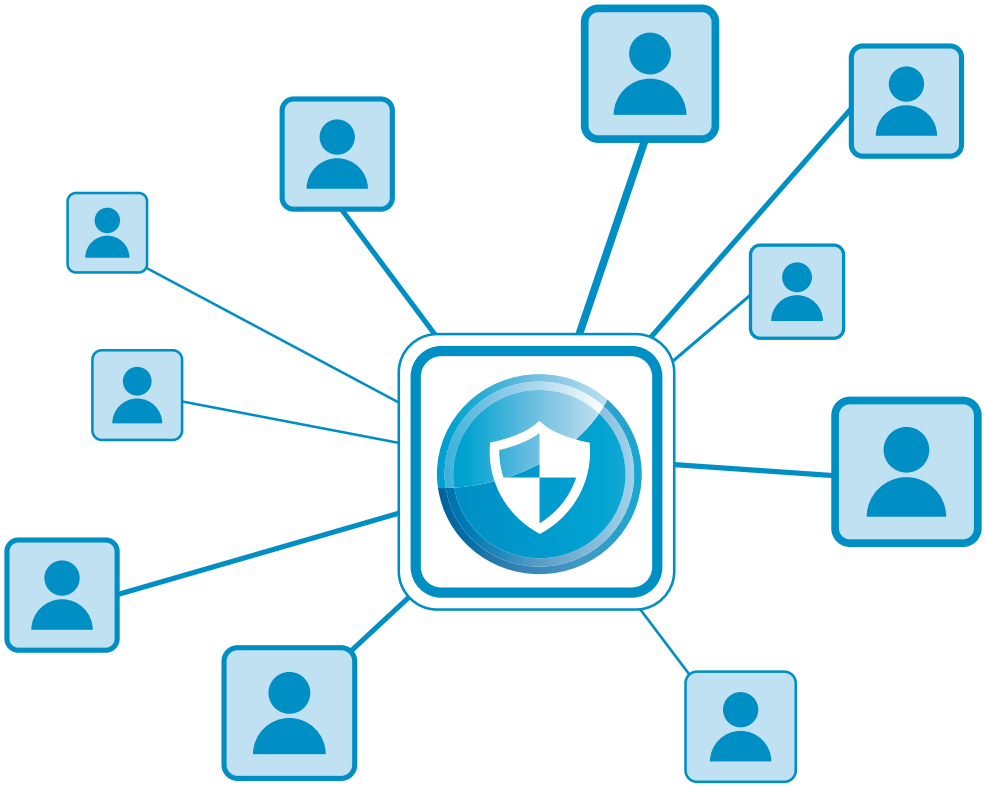
In some countries calls to residential lines do not clear immediately if the called party hangs up. This allows users to hang up and then pick the call back up at another phone that is more conveniently located.

Call Clearing Fraud is a type of impersonation fraud which utilises this delayed cleardown.

The above fraud cases rely on the user being encouraged to perform some action rather than on weaknesses within the core telephony network itself.

Historically telephony networks were formed on the basis of trust between a relatively small numbers of network operators. The technology that the networks used (recently SS7) was secure as it was both physically difficult to access and technically difficult to understand.

The move to modern IP-based networks has changed everything.



Today's Telephony

There have been two key developments in the telephony industry that mean networks are no longer as secure as they used to be:

Liberalisation of the telecoms market

Whilst liberalisation has brought competition to the telecoms market bringing with it reduced costs and improved levels of service, it has also led to inherent security weaknesses.

While it is easy for a small number of incumbent operators to maintain security within their networks, it becomes a very different situation when a large number of smaller networks start springing up. In general these new networks, particularly the smaller ones, are more focused on making a profit than ensuring that their network is secure. As such, network systems may be left misconfigured or unauthorised devices may be connected to the network for malicious purposes.

Of course with SS7 networks, there is still the technical challenge of getting these network systems configured. Despite an increased demand for network engineers, there are still only a limited number of such engineers that have the skills to commit fraud on a TDM SS7 network.

The move towards IP everywhere

IP transmission and packet-based switching equipment is significantly cheaper when compared to TDM transmission and equipment. This has resulted in a drive towards using IP-based technologies everywhere in the network.

On the telephony side, this has resulted in a move away from SS7 over TDM bearers to SS7 over IP (SIGTRAN) and on to SIP.

While SS7 over IP increased accessibility to hackers, the use of SS7 still presented challenges. However the use of SIP brings with it new, unknown challenges that need to be addressed. While SIP may thought of as being secure, there may be new and emerging weaknesses that are not known about yet. Once they are they will be exploited to commit fraud.

Network admins appreciate the flexibility of being able to configure their systems from anywhere.

Once configuration interfaces are exposed to the Internet they become a target for hackers. Even if an interface is thought of as being safe, it may contain security holes that can be exploited.

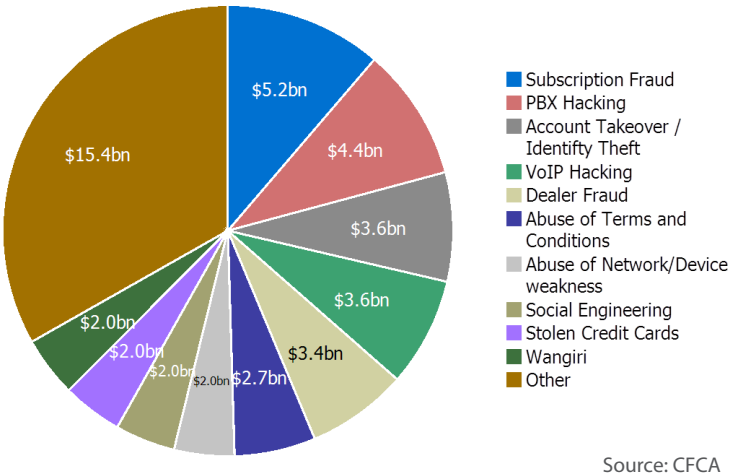
In the PC and server world software and operating systems are regularly patched with security updates in order to prevent hackers exploiting weaknesses. Whilst this strategy is valid for server-based IP telephony systems, the spread of VoIP appliances into enterprise and residential customers means that there will be an increasing number of unpatched devices ready for hackers to exploit.

Telephony Fraud Today

According to the Communication Fraud Control Association (CFCA), fraud costs the telecoms industry 1.69% of all revenues – that is over $38bn annually.

Two of the main causes of fraud are PBX hacking and VoIP device hacking. Together, these types of fraud cost the industry over $8bn annually and account for almost one fifth of all telecoms fraud.

These types of fraud are outlined below:



Source: CFCA

PBX Hacking

Although it is possible to cause PBX fraud, by setting up call forwarding on an extension, PBX hacking has increased following the introduction of SIP telephony and IP PBXs.

The introduction of IP PBXs has led to an increase in PBX fraud. IP PBX's have a management interface which is often connected to the Internet so that the PBX can be managed from outside of the office.

Although the software is not necessarily weak many small companies do not understand the importance of using strong passwords on externally accessible systems. Once a hacker becomes aware of the IP PBX on the Internet, they can target the configuration interface looking for the use of default or weak passwords. If they gain access they can use their access to commit fraud such as using the PBX to commit International Revenue Share Fraud.

PBX fraud can be costly for the network operator as they usually bear the cost of the fraud, as many operators are reluctant to enforce debts, as that may cause damage to their reputation.

VoIP Device Hacking

A number of providers have started offering IP telephony to residential users. Users can then either use a SIP handset or plug their existing telephone into a suitable gateway or router that supports SIP.

As residential use of IP telephony increases, so will attempts to break into devices and steal users' credentials.

Once stolen, a hacker may make calls on the user's account – usually without them even knowing about it until they receive their monthly bill.

As the number of different types of residential VoIP gateways increases this will undoubtedly lead to more vulnerabilities being identified. Although many of these vulnerabilities will be fixed by the vendor, older devices are likely to be left unpatched and many users will not update their devices.

Other Fraud

In addition to these types of fraud which target devices, it is likely that weaknesses will be discovered in the underlying protocols or how network operators implement their connections to other networks.

There have already been examples of calls passing through SIP interconnects without any verifiable caller identification parameters.

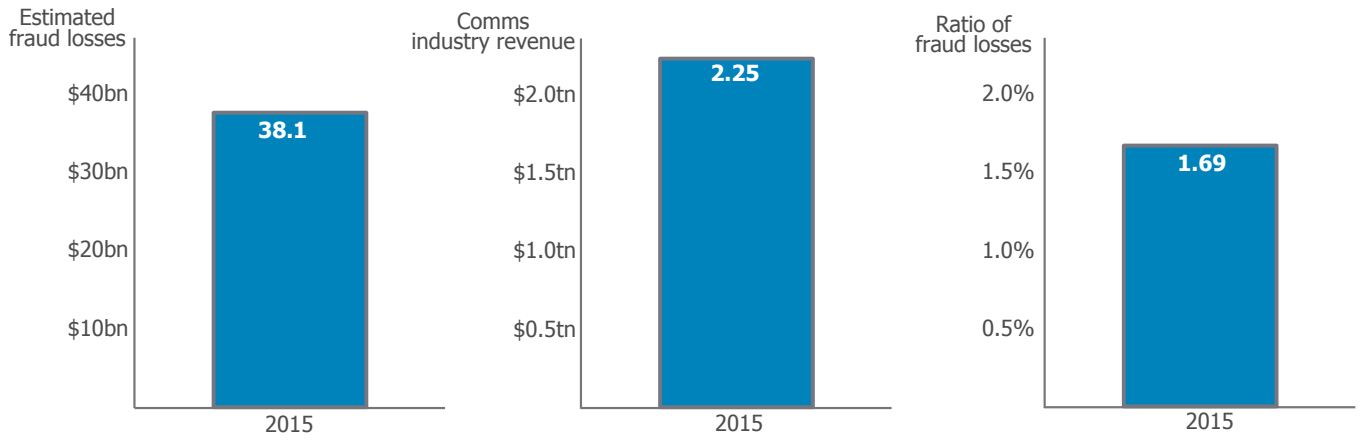
As the use of SIP increases, it is inevitable that new vulnerabilities and types of fraud will become apparent.

Fraud Trends

SS7 based telephony networks were inherently secure due to difficulties in gaining physical access and technical obscurity. Modern IP networks do not provide the same level of physical security – IP is more accessible than TDM – and SIP is more widely understood than SS7. This means that, in general SIP based networks are less secure than SS7 networks were. This weakness will be even more apparent where different networks communicate with each other.

As we enter the world of SIP interconnects, operators will need to implement robust fraud control measures to detect and manage fraud. Otherwise their losses are set to increase.

The ease of configuration of SIP based systems will also lead to an increase in fraud. Whereas it was difficult to configure TDM equipment (often requiring proprietary management tools), configuring VoIP equipment is trivial by comparison. This opens the window for disgruntled employees to make malicious configuration changes to network systems.



Source: CFCA, 2015

How To Prevent Telephony Fraud

While it may not be possible to completely eliminate the possibility of fraud occurring, it can be reduced by early detection and taking steps to block fraudulent use as soon as detection occurs. This is not a one off activity, but should be a continuous business activity, adapting fraud prevention strategies as fraudsters adapt new strategies.

The top steps to preventing fraud include:

1. Understand the nature of the fraud affecting the network

The first step to preventing fraud is to understanding what normal network usage is, and how calls into the network are balanced by calls going out of the network.

Network analysis may be carried out either by studying call detail records, or by installing a system into the network that monitors calls setups and cleardowns, producing detailed call analytics.

2. Detecting fraud

Once the network has been analysed, it is possible to define a number of call rules that are used to define normal network operation, and these may be used to flag up potential fraud – either on a per-user or network wide basis.

Once these rules have been defined, they may be applied to the network, and any calls that break the rules may be flagged up as potential fraud. This allows the rules to be continually refined to gain the greatest level of protection with the fewest false-positives.

3. Blocking fraud

Once the network operator is happy with the call rules, they may switch from detection mode – where calls breaking the rules are flagged up – to call blocking mode – where calls are automatically blocked by the network.

4. Refining filters

Even when the fraud prevention system is actively blocking calls, it is important not to get complacent, and to keep refining the call rules.

As fraudsters notice that routes are being blocked, and they are no longer able to make money from their activities, they will adapt to work around the rules that are being applied to limit their calls. As they adapt their behaviour, it is important to keep analysing network activity to detect how the fraudster is changing their behaviour, and updating rules to keep one step ahead in protecting the network and its customers.

It is also worth remembering that many criminals look for easy opportunities. While adopting fraud prevention strategies may not totally secure a network, fraudsters will look for easier targets, leaving protected networks alone.

Unusual Calling Patterns

Fraud can often be detected by looking for unusual call patterns.

There are a number of ways in which call patterns may be inspected, however the most common method is by analysing Call Detail Records (CDRs). Whenever a call occurs a CDR is generated. This contains details of the call including origination, destination, any call diversion and the call duration.

CDRs may be loaded into a data analytics system which examines the CDRs looking for unusual calling patterns, flagging up any problems to the operators for further analysis. The operator may then perform further checks before deciding if those calls are fraudulent and then adding rules into the telephony systems to prevent further fraud from occurring.

The top 5 calling patterns that may indicate fraud are:

1. Calls at unusual times

Businesses typically operate standard working patterns such that the majority of calls occur between 8am and 6pm.

A large number of calls outside of these hours, particularly to expensive destinations (premium rate or international numbers), may indicate that a PBX account has been hijacked and is being used to commit fraud.

2. High volume of short/failed calls from premium/international originations

A high volume of very short calls from premium rate or international numbers may indicate that someone is trying to commit Wangiri fraud by leaving missed call notifications on phones.

With this type of fraud the fraudster tries to trick users into calling back the missed call number so that they can collect a share of the call revenue.

3. Users making lots of calls to lots of different numbers

In general most users have a relatively small number of peers that they frequently communicate with. This communication is generally bidirectional - they make calls and they receive calls.

If a device is used to make a large number of calls to different destinations and does not receive any calls, then this is indicative of a SIM Box – a computer controlled VoIP to mobile gateway that is being used to commit telephony fraud.

4. Multiple simultaneous calls

Whilst not generally understood it is possible for mobile phones to have more than one call in progress at the same time. The most common use case for this feature is for conference calls, however it can also be used to initiate explicit call transfer. The explicit call transfer service allows a mobile user with two calls in progress to connect those parties together and then drop out of the call.

By using explicit call transfer on a stolen mobile phone the fraudster can initiate multiple IRSF calls that can run up large bills in a short period of time. Such calling patterns are indicative of fraud.

5. Lots of short calls to an expensive number

There is another type of fraud that is called "Fake Answer Fraud". With this type of fraud the fraudster advertises a service on a premium rate number. When a user calls this number, rather than receiving the advertised number, they simply hear ringing or what appears to be a network announcement. What they don't know is that the call has already been answered and they are paying for the call. After a while the caller gets bored and hangs up.

Depending on the nature of the number that has been called the caller may be left with a large bill for the call.

This fraud can be identified by multiple relatively short calls to a premium rate number before the caller clears.

Whilst inspecting past CDRs is useful, it is only a retrospective indication that helps to spot fraud patterns. It doesn't in itself proactively protect against it.

Network operators need a more complete approach to protecting their customers and their networks.

Telsis' Fraud Prevention Solutions

While other vendors look to identify fraud by analysing CDRs, Telsis takes a far more comprehensive appoach.

Post processing of CDRs takes time leaving fraud windows open and contributing to losses. Even after the fraud has been identified, it takes time for network engineers to add rules to block the fraud.

In order to combat the growth in telephony fraud, Telsis offers real-time fraud protection with **Voice SafeGuard**. Voice Safeguard is an in-network solution that analyses calls, records details of call setups and call durations and performs real-time analysis of those calls thus preventing fraudulent calls being made in the first place.

Being integrated within the network and taking a live view, unusual calling patterns can be detected and flagged up far more quickly and once fraud has been detected, Voice Safeguard makes it easy to add rules that block future calls. Voice Safeguard also gives operators the opportunity to tear down fraudulent calls that are in progress rather than simply blocking new calls. Tearing down calls can reduce fraud losses associated with multiple long calls to high cost destinations.

Voice SafeGuard Outbound Call Protection monitors calls made to premium rate and international numbers, applying rules to limit the number of calls and the call duration of calls that may be made to different destinations, both from an individual telephone number and globally through the network. Different limits may be applied at different times of the day in order to handle both working and non working hours.

Voice SafeGuard Interconnect Policy Control polices connections with other network operators. Although Session Border Controllers provide a good level of protection against some types of signalling level security threat, they do not protect against network fraud.

Voice SafeGuard is continuously being developed in order to protect against new and other types of fraud. This ensures that network operators are able to provide the best level of protection for their customers.

Telsis has over 28 years of experience working with network operators to provide robust solutions that help them to protect and grow their revenues.

Glossary

Acronym	Term	Definition
CDR	Call Detail Record	A record of call that is used for billing purposes and may also be used for analytical purposes
CLI	Calling Line Identity	A telephone number that indicates the origin of a call.
IP	Internet Protocol	A protocol for transferring data between two end points on a network
IRSF	International Revenue Share Fraud	A type of fraud involving premium rate numbers in different countries
NFV	Network Function Virtualisation	A network architecture using IT virtualisation technology to create telephony networks
PBX	Private Branch Exchange	A small telephone exchange device that serves a particular business or office
PRS	Premium Rate Service	A telephone service where the call charges are higher than normal call charges
SDN	Software Defined Network	A network architecture where the control and management of the network is split from the actual network devices
SIGTRAN	Signalling Transport	A technology for transporting SS7 signalling messages over an IP network
SIP	Session Initiation Protocol	A next generation telephony signalling protocol
SS7	Signalling Scheme No. 7	A telephony signalling protocol that is used within and between TDM telephony networks
TDM	Time Domain Multiplexing	A method of transmitting multiple telephone calls over a single physical data link. Information for each call is given a fixed period of time, and the time periods are multiplexed together
VoIP	Voice over IP	A technology for carrying calls over an IP network

www.telsis.com

Email: contactus@telsis.com

UK
T: +44 (0) 1489 76 00 00

Germany
T: +49 (0) 6151 827 850

Telsis