



Hacker Trac IDM

Protect the vulnerabilities in your PBX with IDM

Helps prevent fraud

Helps prevent hacking

Helps prevent abuse

PBX Toll Fraud Protection

PBX Hacking and Toll Fraud:

Telecom fraud costs business billions of dollars annually and there is every reason to expect the trend to continue. A key selling feature of even the smallest business phone system is that it can be networked with everything else in the office. Most IPT PBX solutions are based on a standard PC server configured with either Open Source or proprietary IPT PBX software. They connect to the Internet for the purpose of transmitting both voice and data along the same circuit. Ironically, while most of us would not consider connecting a PC to the Internet without a firewall and anti-virus software the same caution apparently does not apply to the installation of an IPT PBX. It is ironic because the exposure is in fact probably greater.

It is for these reasons that the role of PBX call accounting software has changed significantly in the transition from TDM to IP technology. In the past voice and data communication rarely touched one another. Today cohabitation is the norm. They are comprehensively entangled within packets that share the same LAN and WAN as the PBX and IT servers. In the transition from analogue to digital and from PSTN to IP the business phone system has become a far more useful piece of technology but it's also more vulnerable than widely appreciated.

Signs of Fraud

Symptoms of phone fraud that trigger the attention of Teltrac's IDM software include:

- Calls to maintenance ports.
- Direct Inward System Access (DISA) calls.
- Call forwarding
- Calls to unexpected and unusual destinations
- Out of hours calls
- War dialing – large volumes of in-bound short duration calls
- Network breakout calls – trunk to trunk
- Calls that exceed thresholds: duration, cost or volume

As cases of phone fraud become more common expect to see a resurgence in the use of telecom expense management systems.

Fraud Prevention Tool

HackerTrac Intrusion Detection Module is a comprehensive security and "anti-hacker" system designed to protect your communications assets by monitoring and analyzing your incoming and outgoing telecommunications traffic in *real time*.

IDM can reveal any abnormal calls or call patterns indicating fraud, abuse or unauthorized usage of your telephone system and broadcast alerts via email, screen pop, text ... to nominated personnel while the event is in progress..





HACKerTRAC

- Real time fraud monitoring of calls and traffic within your network
- Alarms to e-mails, pagers, pop-up screens
- Time defined alarms
- Country defined alarms
- Traffic pattern alarms
- Daily value alarms
- Number defined alarms

Technical Requirements

Teltrac (any version) with SQL Server

How can you protect your telephone system?

As your company has to continue working and use your phone system in the most liberal manner that suits your way of doing business, the best way to prevent hacking is not by reducing the capabilities of your system but by putting in place a protective solution that enables you to recognise instantly any abnormal calls or call patterns.

How does it work?

At your server site: Collect the Call Logging Data from all your different PBX within your network. Immediately process and validate all your Call Data. Set alarm levels deliverable by e-mail or SMS instantly as they occur.

EMPLOYEE ABUSE CONTROL ALARMS

- Alarm when a specified number is called (e.g.. sex number)
- Alarm for a call over a specified charge for any specified country at a specified time
- Alarm for a call over a specified duration for any specified country at a specified time
- Alarm when call is made to a specified country

FRAUD DETECTION ALARMS

- Alarms for a call made at a specified time of the day (e.g. from 11pm to 6am)
- Alarm for calls from unrecognized FAC/DISA/Authorisation ¹
- Alarm for calls from same FAC/DISA/PIN code from more than one location ^{1,2}
- Alarm for outgoing calls made from certain extensions (voice mail extensions)
- Alarm for calls to/from unlisted extension, unlisted trunk
- Alarm for calls to maintenance ports
- Alarm for any DISA calls (for systems where DISA is supposedly disabled) ^{1,2}
- Alarm when the number of calls per PBX per day exceeds a certain pre-defined number
- Alarm when total call value per PBX per day exceeds a certain pre-defined value
- Alarm for spikes in call count or total call durations for a given extension or trunk
- Alarm for repeated dial attempts to a given DISA trunk ^{1,2}
- Alarm for DISA calls being made using FACs of people known to be currently inside the office ^{1,2}
- Alarm on "WAR" dialing for attempts to find a flaw in the system by calling numbers sequentially ²

INTRUSION DETECTION REPORTS

- Trunk detail and trunk summary reports
- Call journal & Alarms settings review report & Alarms log report
- Report on most frequent incoming callers (to identify attempts to dial in to all PBX numbers to find an entry point)

1. AUDIT Auth/DISA Module required
2. ICM Inward Calls Module required
3. All items subject to PBX CDR data content

HACKerTRAC IDM & TELTRAC, a complete solution:

Intrusion Detection is an essential item of network administration today. In addition, a full and complete management of your voice and data network can be achieved by implementing a TELTRAC Call Management System:

- Full Call management reporting capabilities (100's of reports available) to control, manage and allocate the costs and facilities of your network.
- Standalone or Multi-site call management and accounting for up to 100,000 extns / 256 PBX on a single Wintel server.
- Voice Private Network logging to consolidate and bill back precisely the different branches of your corporation on their usage of VPN investment.
- Out-source servicing: whether for your call management or your alarms management Interpac's Teltrac Outsourced Managed Services provide call logging for your network 24 hours a day from our service centre in Hong Kong.

Teltrac, Multi-Trac and Trac-Record are all trademarks of Interpacific Data Management Limited.