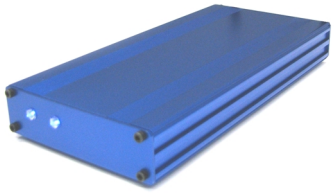
FraudCatcher ® Telecom Fraud and Surveillance System



FraudCatcher is a next-generation fraud detection and prevention system that is capable of identifying and thwarting a wide range of sophisticated attacks before losses occur. Developed from the ground up this next-generation system is designed to detect and stop fraud incidents in near real-time.

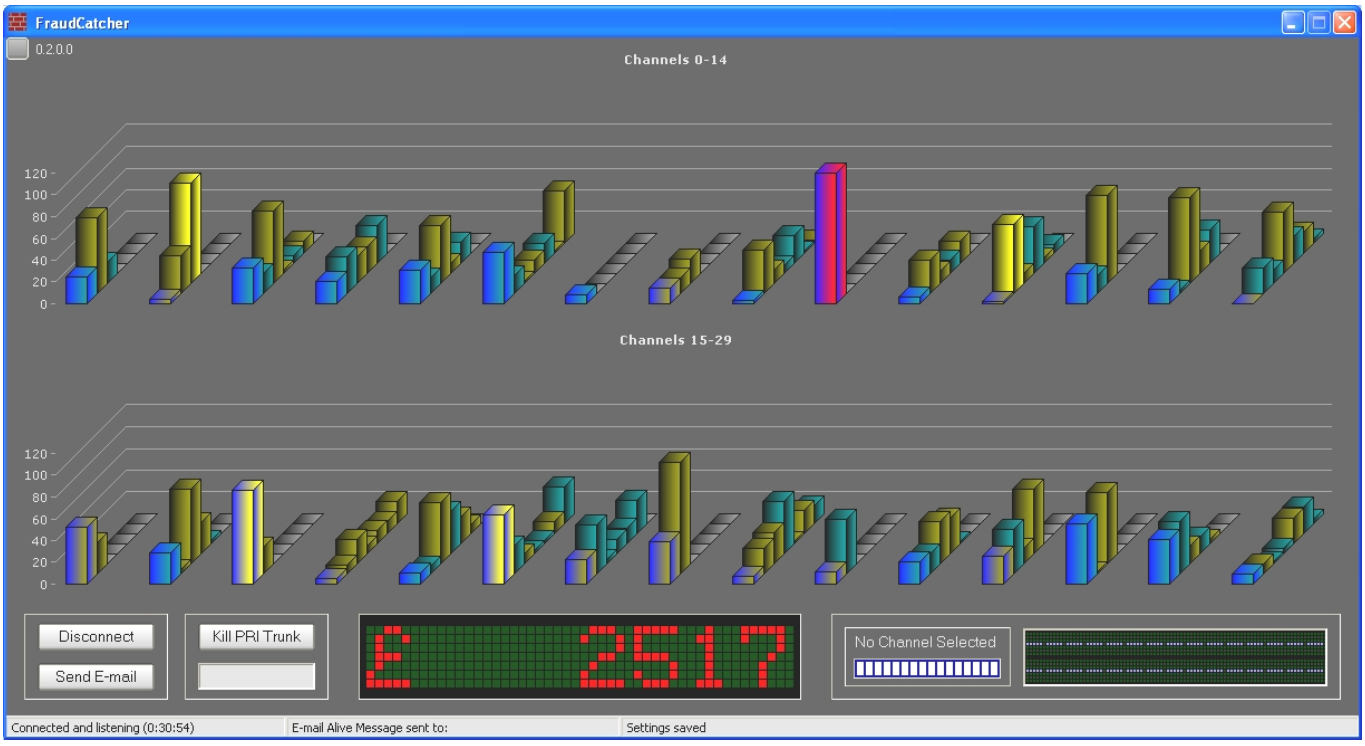
Real-time analysis

Unlike conventional CDR analysis solutions, which simply examine switch call records after the fact, **FraudCatcher** fraud detection and prevention system uses a passive network probe to pro-actively and continuously analyze telecoms traffic in real-time. **FraudCatcher** BRI ISDN-2 and PRI ISDN-30/DASS2/DPNSS/Q.SIG are installed in the enterprise to detect attacks aimed at the business. Once an attack is detected, the fraud management system may instruct the interface to drop the line.

Audio snapshots by E-mail

Each E-mail alert includes all relevant call details and timings of the call in progress (CLI, DDI, Dialed Outbound Number and the cost sofar).

Additionally it can have a sample audio recording file attachment for immediate replay by the E-mail recipient in order to verify if a call, that appears to be out of bounds, is a genuine call or a fraudulent call. **FraudCatcher** can be configured for either manual or automatic intervention in order to stop the attacks.



Alert Type examples

Blacklist - receive alerts when traffic to/from blacklisted sources is detected in the PBX:

- Number Blacklist - Set up your own list of blacklisted numbers.
- Community Blacklist - Protect your PBX from industry confirmed blacklisted numbers.
- Country Blacklist - Receive alerts when traffic to/from specific countries you select is detected.

Timestamp - receive alerts when calls originate from your organization at suspicious times.

- User defined time ranges.
- Holidays.
- Business hours.

Phishing & Threshold - receive alerts when hourly, daily or monthly costs, durations, or call volume thresholds are exceeded. Apply to specific numbers, to specific countries, or to overall traffic.

Types of Telecom Fraud

Premium Rate fraud
Owners of premium rate telephone numbers profit from hacking into PBXs around the world and routing calls to their own premium rate services.

Call Sell PBX Fraud
Online or offline call wholesalers hack into PBXs in order to sell calls to their customers without incurring any of the charges themselves; the more expensive the destination the better; the more calls the wholesaler can route out of an organization simultaneously the better.
Destinations may be satellite phones that cost £8/minute to call, or countries that cost upwards of £2/minute to call. Obviously, the more lines the fraudster uses to perpetrate the attack, the more profound the financial loss.

PBX Dial-Through
Dial-Through fraud relies on DISA (Direct Inward System Access) features that exist on every PBX. These features allow employees to call into the switchboard or their voicemail and make outgoing calls after inputting a password or pin. Although this feature may be turned off upon installation, hackers will try to break in and create their own mailbox which will allow them to dial in and then make any calls they wish.

Calls to Known Fraudulent Destinations
Telecom fraud is a well-known problem, and there are blacklists of phone numbers, area codes etc., that can be blocked or monitored.

Out of Hour Calls
Calls originating from an organization's PBX may be the result of Internal Employee Fraud, unauthorized visitors, or remote hackers accessing the system. Most significant telecom fraud attacks are perpetrated when the enterprise is unmanned at night, over weekends, bank holidays, religious holidays, etc.

Internal Misconduct
Telecom fraudsters are not always outside the confines of the organization. Internal Employee Fraud is a significant contributor to fraud affecting organizations. Employees may use company phones to make premium number, personal, and long distance calls. In the worst case scenario employees may actively enable toll fraud. It is possible to program an internal phone to autoforward to an international destination or to create a mailbox with dial-out privileges allowing the employee to call it at local rates while forcing the company to pay the long distance charges.

Background

According to the Communications Fraud Control Association 2011 Global Fraud Loss Survey, over $40.15 Billion are lost each year to telephony fraud. Three important sources are PBX/Voicemail Hacking ($4.96 Billion), Dial-Through or By-Pass Fraud ($2.88 Billion) and Premium Rate Service Fraud ($2.24 Billion). According to the survey, 98% of participants felt that global fraud losses had increased or stayed the same, while 89% said fraud has trended upwards within their company.

The Report cites:

The top five countries where fraud originates:

United States, India, United Kingdom, Pakistan, and the Philippines;

The top five countries where fraud terminates:

Cuba, Somalia, Sierra Leone, Zimbabwe, Latvia;

Company information

Voice2record specializes in fraud detection and voice recording products for use in analog, BRI, PRI and SIP infrastructures and has its office in Amsterdam at 25 minutes from Schiphol International airport.

De Cuserstraat 93, 1081 CN, Amsterdam,
The Netherlands

www.voice2record.com
info@voice2record.com

VOICE2RECORD