SANDVINE

Interconnect Bypass Fraud Management

Protect your network from fraudulent calling services

INTERCONNECT BYPASS FRAUD MANAGEMENT DELIVERS:

Advanced Fraud Detection
Detect and prevent attempted fraud leveraging Sandvine's extensive library of application signatures focused on fraud detection

Preservation of legitimate voice revenue
Ensures that the operator receives revenue for the services that they are providing to users with voice services

Blocking of illegal voice service bypass
Blocks attempted circumvention of interconnect services designed to deprive an operator of their legitimate revenue

MARKET OVERVIEW

In the telecommunication world, fraud is usually defined as the abusive usage of network and services without the intention of paying for the services or the theft of telecommunication network services. All types of telecommunication frauds are damaging to the network operator's revenue.

A new type of fraud that is affecting operators is OTT bypass fraud, which is based on legacy interconnect telecom systems. OTT bypass fraud, also known as interconnect bypass fraud is a growing challenge that network operators around the world are facing. According to a recent survey by the Communications Fraud Control Association, interconnect bypass fraud is one of the largest sources of lost revenues and costs network operators across the globe an estimated $4.3 billion (USD) annually.

Interconnect bypass fraud is lucrative due the fact that phone companies have agreements with each other where they pay a fixed interconnection fee for any international call that passes through or terminates within their network. For example, a call originating in the United States but destined for Brazil could travel through networks in Mexico and Colombia before reaching the end user. In this instance, a portion of the per minute fee paid by the user would go to each of the networks the call passes through.

Until recently, the majority of interconnect bypass fraud was attributed to "SIMbox fraud," which involved installing a piece of hardware known as a SIMbox into the interconnect within a public switch telephone network (PSTN) to bypass traditional voice call routing. A SIMbox contains many SIM cards which allow a fraudulent actor to intercept calls and collect the majority of the interconnect fees as their SIMbox forwards these calls over a lower quality mobile connection. Due to the explosion of mobile VoIP applications, another interconnect bypass fraud has emerged called OTT bypass fraud in which a normal phone call is diverted over IP to a mobile VoIP application on a smartphone, instead of being terminated over the normal telecom infrastructure.

SANDVINE SOLUTION

By using the advanced heuristics and machine learning capabilities of the Sandvine platform and vast OTT signature library, the Sandvine solution is able to differentiate between authorized OTT VoIP apps from fraudulent OTT VoIP app calls. With this understanding of varying call types, Sandvine uses Active Network Intelligence to break out the composition of OTT VoIP apps. These calls can be blocked or logged. Triggers can also be set to send notifications to the users of fraudulent applications. This data can also be used to track and block the illegal bypass services to ensure that other users are not defrauded or delivered substandard services from which the operator may suffer reputational harm.

Sandvine's frequently updated signature database ensures accurate identification of attempted interconnect bypass fraud and enables active management to prevent fraud

UNIQUE VALUE PROPOSITION FOR DATA FRAUD MANAGEMENT

Sandvine is the leader in VoIP and fraud management. The Sandvine solution for VoIP-related fraud provides the broad functionality and flexibility needed to deliver reliable compliance and protection against fraud, while also preserving the ability to adapt to changing fraud techniques, traffic makeup, and patterns of usage.

The solution is provided with an extensive application signature library that is continually updated to identify new and changing applications including encrypted application traffic. Through extensive use of behavior analysis, heuristics, and machine learning, Sandvine can detect VoIP applications that are attempting to hide from detection from regulators and the network operators. For region or country-specific fraud services, Sandvine works directly with network operators to design custom signatures to capture all types of fraud offerings.

The Sandvine Interconnect Bypass Fraud Management solution enables operators to both save money as well as make money in the following ways:

Save Money

- CAPEX savings by eliminating usage that affects network capacity
- Penalties paid to regulatory authorities for failing to filter voice services violating governmental usage policies

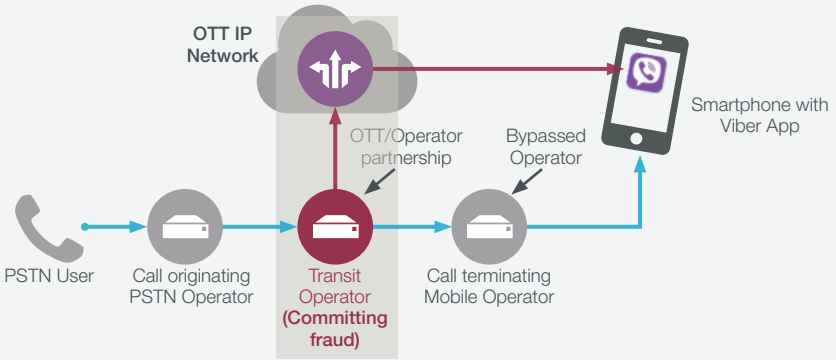
Make Money

- Revenue recovery for fraudulent voice services delivered by fraudsters
- Revenue recovery for interconnect PSTN transit fees

Sandvine's rich visibility and reporting visualization with our Insights products ensures that the operator can see the scope of the interconnect bypass fraud that is occurring on their network, and then determine the proper actions to take. As shown in the example below, legitimate OTT VoIP applications can be used to deliver fraudulent voice service offerings that bypass the safety and security needs of users:

Figure 1

Viber-in allows individuals to receive "incoming calls from non-Viber numbers" and fraudulent actors have replicated the SIMbox scenario by using Viber-in service in place of SIM cards



ABOUT SANDVINE

Sandvine helps organizations run world-class networks with Active Network Intelligence, leveraging machine learning analytics and closed-loop automation to identify and adapt to network behavior in real-time. With Sandvine, organizations have the power of a highly automated platform from a single vendor that delivers a deep understanding of their network data to drive faster, better decisions. For more information, visit **sandvine.com** or follow Sandvine on Twitter at **@Sandvine.**

SANDVINE

USA
2055 Junction Avenue
Suite Number 105
San Jose,
CA, 95131
USA

EUROPE
Svärdfiskgatan 4
432 40 Varberg,
Halland
Sweden
T. +46 340.48 38 00

CANADA
408 Albert Street,
Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

ASIA
RMZ Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333