Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 9, Issue 6

Averting Modern Telecom Scams: Fraud Prevention in a VoIP World

By Alex Hoffman

Telecommunications fraud is a significant concern for communications service providers. It robs carriers of revenues, consumes valuable network resources without remuneration and leads to customer disputes and churn. A 2011 Communications Fraud Control Association (CFCA) survey estimated global telecommunications fraud loss at $40.1 billion (USD), or nearly 2 percent of worldwide telecom revenues.

Next-Gen Networks Are Susceptible to a Myriad of Scams

Today's telecom networks and services are susceptible to many different types of fraudulent activity. VoIP introduces a variety of new security challenges for service providers and opens the door to an assortment of new scamming opportunities for fraudsters. Next-generation fixed and mobile networks are vulnerable to a wide array of increasingly sophisticated attacks: some are based on traditional TDM/PSTN schemes, some leverage newer computer-hacking techniques and some exploit specific VoIP vulnerabilities.

Telecommunications fraud can come in many forms, and communications service providers need to be both aware of and vigilant about current scams. Some schemes are intended to bypass service-provider networks to avoid normal payment systems for international calls, while some are intended to leverage service-provider networks and sidestep payment. In the most common scheme, attackers exploit insufficiently protected PBX and voicemail systems; fraudsters will initiate calls to revenue-share numbers operated by them at the cost of the PBX owner.

Many scams are aimed directly at the enterprise, but they too can have a significant impact on the service provider. Typically, businesses don't realize they've been scammed until after they receive their monthly bill. Then they can refuse to pay the fraudulent charges, threaten to switch carriers and leave the service provider holding the bag.

A recent AT&T case in which fraudsters hacked into the PBX of a Massachusetts company and made $900,000 in calls to Somalia serves as a good example. The small-business owner refused to pay his bill, so AT&T initiated a $1.15 million lawsuit against him. But after the Associated Press picked up the story AT&T dropped the suit, eating the costs and the bill while creating a negative customer experience and negative perception in the marketplace to boot.

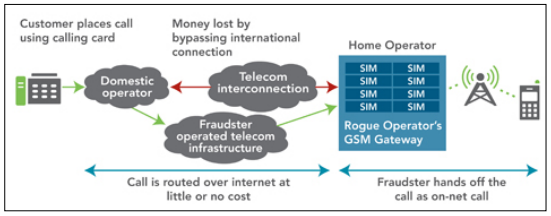
Service providers that incorporate fraud protection features into their offerings and maintain a knowledgeable support staff are, in fact, able to differentiate their PBX service offerings. In some markets PBX customers expect their service providers to proactively prevent fraud and cover any fraud-based losses if they occur.

Here are the more common scams to look out for:

- PBX/voicemail hacking and call-transfer schemes, like the Massachusetts case in which fraudsters gained access to an enterprise PBX or voicemail system (or, in some cases, the softswitch in the service-provider network, albeit indirectly) for the purpose of making free long-distance or

international calls. In more sophisticated versions of the scam, rogue service providers "resell" the services to their own subscribers or place calls to their own premium numbers to collect termination fees (revenue-share fraud);

- Traffic-pumping schemes, in which rogue carriers strike traffic-steering deals with conferencing services or adult entertainment services, or in which subscribers are duped into placing calls to premium-rate services;
- Bypass fraud, in which SIM boxes (GSM gateways) are used to circumvent standard network interconnections and avoid the normal payment systems for international mobile calls. In one popular mobile calling scheme, fraudsters sell inexpensive overseas calling cards to expatriates and illegally route international calls across the Internet or a VoIP network to a GSM gateway for handoff to a local mobile-service provider. By making internationally originated calls appear as on-net mobile-to-mobile calls, these schemes rob the home mobile operator of standard international connect fees while creating QoS and spectrum management issues. A rash of SIM-boxing schemes has made international headlines over the past several years; in Ghana, for example, investigators have recently broken up dozens of scams, most involving hundreds of SIM cards, which were believed to have cheated local mobile operators out of millions in monthly service fees.



Conventional Techniques for Combating Telecommunications Fraud Fall Short

Many service providers still rely on inefficient and rudimentary practices for fighting fraud, including:

- Call blocking, in which the provider simply rejects calls to countries with high incidences of fraud (Cuba, Somalia, Sierra Leone), forfeiting legitimate international calling revenues;
- Third-party routing, in which the provider routes calls to high fraud countries through intermediary "validation service" operators, who verify call legitimacy at additional expense;

Australia's Defence Signals Directorate blocks 85 percent of cyber attacks with four effective methods.

- Call Detail Records (CDR) analysis, in which switch call detail records are scrutinized for unusual calling patterns. While basic CDR analysis can help identify or isolate certain types of service theft, it typically cannot be used to detect or prevent acts of fraud in real-time (as the aforementioned roaming-fraud example illustrates); service providers can lose millions before a threat is discovered and contained. Worse still, conventional CDR analysis tools aren't capable of detecting contemporary threats like IP reconnaissance scans, which hackers often use to identify and exploit security weaknesses in VoIP networks.

Many service providers are looking for more efficient and comprehensive ways of detecting and combating attacks before they proliferate.

Next-Generation Fraud Management Systems Put an End to Complex Scams

Forward-looking service providers are implementing next-generation fraud detection and prevention systems that are capable of identifying and thwarting a wide range of sophisticated attacks before revenue is lost. Developed from the ground up with VoIP in mind, next-generation systems are designed to detect and stop fraud incidents in near real-time.

Unlike conventional CDR analysis solutions, which simply examine switch call records after the fact, next-generation fraud detection and prevention systems use passive network probes to proactively and continuously analyze network traffic in real-time. Probes can take the form of standalone devices, or they can be embedded into other network elements such as session border controllers (SBCs). For ultimate protection, probes are installed in both the enterprise and service-provider network to detect attacks aimed at either the business or the carrier infrastructure. Once an attack is detected, the fraud management system may instruct SBCs or other network elements to drop or block suspicious calls.

Behavioral Analysis Tools Detect Unusual Calling Patterns

While fraud attacks have different faces, the

symptoms tend to be the same, namely a deviation in a user or user group's normal behavior. Common attack symptoms include:

- Unusual ratio of incoming to outgoing calls
- Unusual number of night or weekend calls
- High volume of calls to distinct numbers
- High volume of call redirects from voicemail
- Unusually high volume of subscribers on one cell (SIM boxing)
- Unusual ratio of on-network to off-network calls (SIM boxing)
- Absence of SMS or data traffic (SIM boxing)

Best-of-breed fraud management systems provide flexible rules and scoring systems that enable administrators to set policies, customize actions and weed out false positives. By analyzing network calls over time and learning the behavioral patterns of individual users as well as user groups, next-generation fraud management systems are able to detect the unusual calling patterns that are symptomatic of telecom scams. And since they collect and analyze data over time, the longer they are installed, the more accurate and effective they become.

Collaborative Blacklisting

Information sharing between service providers can facilitate a form of fraud prevention known as blacklisting. Attackers locating holes in telecommunications infrastructure and fraudsters abusing the system may not be the same person. Stolen account information is sold over the Internet to fraudsters who design and execute scams. An enterprise or service provider may be hit by fraud without seeing fraud precursors such as scanning activity from the same source before. This makes information sharing between service providers much more relevant. Adding small bits of information from multiple providers helps to paint a bigger picture and prevent fraud before it happens. Information worth sharing includes source IP addresses of attackers, phone numbers dialed during the reconnaissance phase or technical details such as the client software used to initiate calls. In a blacklist approach this information can be incorporated into a fraud detection and prevention system (FDP) to identify and block known scams.

No account should have both administrative access and access to networks outside of the organization, including the Internet and email.

Next-Gen Networks Require Next-Gen Fraud Protection

Communications fraud costs service providers billions of dollars per year. Today's VoIP networks are subject to increasingly sophisticated and costly attacks that cannot be mitigated in a timely fashion using traditional fraud monitoring techniques. Forward-looking providers are turning to next-generation FDPs to proactively identify and suppress attacks. By quickly isolating and containing scams, next-generation fraud management systems help service providers avoid service theft, prevent revenue loss and reduce customer dissatisfaction and subscriber churn.