Cyclix Networks & Fraud Prevention

Peter Sandstrom, CEO, Cyclix Networks

Rev—180807

Moving telecommunications from the legacy circuit-based model of the past to Voice over Internet Protocol packet telephony (VoIP) has opened the door for business users to enjoy enhanced methods of communication that previously were only imagined.

With these new capabilities come new responsibilities. In particular, one area that must be addressed in this VoIP universe is fraud. An organization's telecom traffic traversing the Internet presents new opportunities for hackers to take advantage of weak security.

Fortunately, there are technical solutions to this problem that can keep criminals out of a company's packet telecommunications infrastructure. These solutions start with the VoIP carrier.

Types of phone fraud

- **IP-PBX proxy-point fraud—**
  If an enterprise PBX has administration access via the internet, and the password is weak, it is vulnerable. Once the black-hats crack the password, they can take control of the PBX and use it as a proxy point to launch expensive calls through the company's system.

- **IP-PBX call-origination fraud—**
  In this form of theft, the black-hat gains access to the corporate phone system and then begins launching calls to sites that pay the thief reciprocating compensation funds for termination. In observing this form of theft, one sees very long calls made to foreign locations. Calls originating in the USA often terminate at locations in the Virgin Islands.

- **Phone-Cracked—**
  In this scenario, the black-hat, generally through brute-force attacks, obtains the login and password of an actual desk phone, then uses that login to connect to the company's hosted carrier to make very expensive calls to foreign locations, on the company's bill.

- **Phone-Denial of Service—**
  Running a hosted phone unprotected by a VoIP-aware firewall leaves it and the entire associated phone system vulnerable to discovery via bulk port scans. Hackers then bombard the compromised phone system with calls, tying up phone lines and rendering them useless to the business until a ransom is paid to regain use of the phone system.

VoIP fraud can render a company's VoIP telephone service completely unusable or result in enormous phone bills due for payment immediately upon receipt.

Fortunately, there are some in the industry that understand the severity of the problem and have acted to do something about it. Cyclix Networks has invested a significant amount of resources to combat VoIP fraud.

VoIP Fraud Prevention Programs at Cyclix Networks

Credit-Watch™—

The vast majority of VoIP carriers leave client accounts wide open with respect to credit, allowing the client to dial and accrue any billing level without limitation.

Cyclix Networks' Credit-Watch™ monitors accounts in real-time comparing dialing against a previously established credit limit. If the customer's PBX or phone should become compromised, Credit-Watch™ contains the fraudulent billing to a very small and manageable amount. Cyclix Networks Operations Center is then alerted with an alarm and the customer is notified that their VoIP system has been compromised

Fraud-Buster™—

Often times, hackers will elect to terminate calls in foreign locations with very high per-minute rates. Cyclix Networks' Fraud-Buster™ watches for dialing to these high-cost foreign destinations, determining whether to allow the traffic to terminate or not. If Fraud-Buster™ triggers with a positive event, international dialing is immediately blocked, and the Cyclix Networks Operations Center is alerted with an alarm. The customer is also notified of the incident.

Fraud-Buster™ has a great track record, saving Cyclix customers hundreds of thousands of dollars in illegal dialing charges over the years.

Tangent™—

Both Credit-Watch™ and Fraud-Buster™ are back-office services that run on Cyclix switching facilities, and so are available to all Cyclix clients at all times on the Network.

However, one more line of defense is required to complete the set of services needed to make VoIP safe and risk free. The third service offered is called Tangent™ and is deployed right at the customer's site. Tangent™, what is known in the VoIP industry as an Application Layer Gateway (ALG), is a device that understands VoIP protocols.

Tangent™ knows how to let authorized VoIP users use the service, while simultaneously turning away unauthorized fraudulent users. Tangent™ knows where the valid switch points from Cyclix are located, and so will allow only those switching points to communicate VoIP with the client's VoIP devices. Conversely, a rogue VoIP signaling source from a fraudster will be ignored and will be unable to infiltrate VoIP devices sitting behind Tangent™ at the customer's site. The hacker will simply have no access to the client's VoIP infrastructure, and will be unable to commit fraud at the client's expense.

Tangent™ is an option on all Cyclix Dial-plans and can be made available to all Cyclix customers installing their own VoIP systems. For Cyclix Business-Connect customers, the security features of Tangent™ are built in as an integrated part of the product. With all Cyclix VoIP products total VoIP security can be realized for any customer on the Cyclix network.

To recap VoIP security options available through Cyclix Networks—

- **Credit-Watch™—**real-time watch of credit limits
- **Fraud-Buster™—**real-time watch of suspicious and fraudulent dialing patterns
- **Tangent™—**real-time VoIP discrimination of access at the customer site

These three services running together on the Cyclix network have, in essence, eliminated fraud from the entire Cyclix customer base. This has resulted in our clients being spared hundreds of thousands of dollars in fraudulent traffic billing. Further, it has allowed our clients to move forward and reap all the other benefits IP packet telephony has to offer today's enterprise, without worry of VoIP fraud.