



## **Anatomy of a VoIP Attack**

By Brendan Ziolo

Most experts have agreed that it was a question of when, not if, a VoIP attack would occur. It was recently reported that the owner of two small Miami VoIP companies was arrested for an alleged \$1 million scam to defraud Internet phone providers.

Authorities charge that the networks of third-party VoIP providers were hacked into and customers' calls were routed over these lines while the perpetrator collected fees from customers without paying fees to network providers. Without a doubt this case is the most public example of what we, in the industry, knew was coming. But now all we can do is look at what transpired and learn how to protect against future exploits.

### **How it happened**

The alleged fraud is actually based on a valid business model. A smaller VoIP provider buys discounted minutes from a larger provider and resells them to its customers at a mark-up or minutes are exchanged between providers as they route calls over each other's networks.

In this case, phone cards were sold but when these calls were routed over the third-party network other call prefixes were used so that his company was not charged for the calls. Basically, revenue was received for the calls, but fees were not paid to the provider for the call traffic, and profits were pocketed to the tune of \$1 million.

Two key hacking techniques were used to make this scam a reality. First off, valid call prefixes needed to be secured so that the network would recognize them. These were discovered by launching a brute force attack against the call servers where a machine would generate and test each potential prefix while recording which ones were valid. This could take a long period of time but once a valid prefix is discovered it can be used for the code's lifetime.

With these codes in hand, a router was then reconfigured and compromised to route the calls across the provider's network using the stolen prefixes for authentication. Since these codes are valid, the network would see it as a legitimate call but the perpetrator would not be charged as the code is not tied to him in anyway.

At the same time, the perpetrator would also ensure no traceability to him by using different techniques such as IP eliminator or proxy servers. This makes it more difficult for authorities to identify the perpetrator when and if the fraud is discovered.

Sounds simple enough and the reality is that it is not too hard to launch this or other attacks and service abuse, such as denial of service or VoIP spam, with minimal equipment and software that is available for free on the Internet.

### **How to prevent it**

The sad part is that this type of fraud can be easily prevented by using some tried and true security methodologies along with unique VoIP protection techniques. First and foremost, all network providers should ensure their servers and routers are running tested and proven firmware and operating systems including all the latest security patches. As well, they should implement the strongest form of authentication possible and ensure passwords and prefixes are not easily guessed during brute-force attacks. This is all common sense from a security perspective but not always implemented correctly.

But more importantly, network providers need to recognize that VoIP networks are different and therefore require unique protection techniques to prevent fraud and other types of attacks. These sophisticated security techniques include signature anomaly detection to prevent known attacks; behavior anomaly detection to protect against day zero attacks; and verification of anomalous behavior to eliminate false positives and negatives.

To implement these techniques correctly requires complete knowledge of VoIP protocols, call states, call features, media flows, and the interaction between various nodes along with a deep understanding of the vulnerabilities themselves. And it has to be real-time protection with sub-millisecond delay for signaling and a few microsecond delay for media so as not to affect VoIP performance.

In the case of the attack above, a combination of fingerprinting and behavior learning would have protected the VoIP providers and the enterprise against the fraud attack outlined above. In all cases, enterprises need to deploy a comprehensive IP communications security product that offers:

- complete protection with real-time performance
- easy deployment and not be a point-of-failure
- automatic user behavior learning
- network level intelligence
- effective handling of VoIP spam; and
- interoperability with major VoIP infrastructure vendors.

This same product can provide security for other real-time applications as well. Only then can you securely realize the power of real-time IP communications applications including VoIP, IM, multimedia and collaboration.

*Brendan Ziolo is director of marketing at Siper Systems ([www.sipera.com](http://www.sipera.com)), a company that specializes in security for VoIP, mobile, and multimedia communications. He can be reached at 214-206-3210 or [bziolo@sipera.com](mailto:bziolo@sipera.com).*

