

The Truth About SPIT

VoIP spam looms, but no immediate threat

Kurt Eby



Surely you've heard of Spam for Internet Telephony (SPIT): the notorious email nuisance, spam, has been threaten-

ing to migrate to phones since the dawn of VoIP. But as content filters and easy deletion have all but made spam an afterthought for most Internet users, the real-time nature of SPIT makes it an entirely different problem altogether.

Baruch Sterman, founder and CEO of Kayote Networks Inc., sums up the major difference between SPIT and spam: "An email comes in the middle of the night and it sits in your inbox, it's no big deal. But if you get a call in the middle of the night and it rings your phone, then that's a big problem." Similarly, if you get an email at work you can read or delete it whenever you want with little disruption to your productivity, but a ringing phone demands more attention.

New Jersey-headquartered Kayote is a VoIP interconnectivity and interoperability services provider that resolves issues common to the VoIP industry. The company has been monitoring SPIT for years and released a white paper detailing a SPIT Prevention Security Model in June 2005. "The threat of SPIT looms just over the horizon, with the ever growing popularity of VoIP offerings worldwide providing an attractive user base at the disposal of malicious parties capable of mounting attacks with minimal resources and expenditure," reads the report.

Spitters

According to Sterman, the low calling costs of Internet telephony makes it attractive

to telemarketers, or "spitters." With current models indicating that Internet telephony calls will likely be free, the economics of SPIT will allow telemarketers to blanket millions of customers and make their money back if even only a few people respond. But while the cost structure is already in place, the lack of audience has so far kept the problem at bay.

"SPIT in general hasn't been a large issue," says Jordan Socran, senior director of corporate development at Radialpoint, a Montreal-based broadband managed services provider. Radialpoint works with ISPs to manage disruptions caused by SPIT if they arise. "We haven't been getting a lot of calls around SPIT yet," he adds.

Sterman assures that SPIT won't be on the horizon forever. He concurs that uptake of VoIP will make the business model more attractive to spitters, and once networks start peering with each other it will be harder to track down spitters.

Content Matters

So what exactly can be done in the future to curtail SPIT? One thing is for certain, the fight will take place on a different battleground than the clash with spam. "[SPIT's] much more difficult to detect [than spam] because there's no content," says Sterman. "Spam filters usually key off words or pat-

terns, but that's in content so you can run through the content and try and make a decision. In a Voice over IP call there's no content until the call has been answered, and then it's already too late."

However, Sterman says there are a number of calling patterns that can be identified as potential SPIT calls. These include: a high volume of calls, like 50 to 100 calls an hour from a particular number; numerous calls of a very short duration; calls made in sequence, such as 555-1111 followed by 555-1112; a very low ratio of dialed calls to answered calls; or a low ratio of repeat calls to new calls. Sterman would like this type of call pattern information embedded into calls so the end user or the firewall of the enterprise receiving the call will be able to make decisions about call handling. "We're more interested at this point in the method of transferring the information than we are about the information itself," says Sterman.

Currently, other methods of SPIT prevention such as identifying callers before answering are not effective: Sterman says caller ID fields can be configured by anyone with a little bit of experience to represent any number. Although Sterman adds that other identification methods such as belonging to a social network will help people know which calls can be trusted.

In the end, if spitting occurs as often as spam and phones are ringing off the hook, some type of comprehensive solution will be needed. Sterman says network operators should start looking to implement even basic SPIT solutions now. ■