

## ComputerWeekly – Preventing Spam over IP Telephony

By Clive Longbottom, Service Director, Quocirca Ltd

Spam filters can easily be trained to give better than 90% effectiveness with zero false positives, and for those who still suffer from a lot of spam in their inboxes, they are either not updating their spam databases often enough, or they just do not see the value of getting 90% fewer e-mail messages.

There was also a bout of Spasms (spam over SMS) – less of a problem for businesses, where this does not seem to have been endemic, but pretty nasty for many children who find that they get messages asking for a response, and then find that up to £10 has been taken from their mobile account as a result.

Again, this sort of spam should be fairly easy to deal with, but is in the hands of the operators, rather than the user themselves.

How about Spim? Spam over instant messaging has not had a big hit yet, but significant instances of spurious instant messaging sessions are being seen where the user is asked to download a file, which unsurprisingly carries some nasty payload.

One more for the list – Spit. Spam over IP telephony is one which so far, thankfully, is pretty rare, and is low on many suppliers' radars. The problem is that it is completely different to the others.

Spam, Spasms and Spim are all asynchronous to one degree or another – an e-mail can be easily taken out of a queue and held up for a few minutes while analysis is carried out, and no one is going to notice.

The same goes for Spasms. SMS messages turning up a couple of minutes late is no big deal, and for certain providers I could mention, getting them to turn up within the same working day seems to be beyond their powers as yet.

Even with Spim a delay of a few seconds does not detract from the overall efficacy of the discussion session. And if most users are like my daughter, then there will be anywhere up to 20 sessions going on at the same time, so a delay is inevitable.

But Spit is different. If we decide to analyse all incoming calls we have a major problem. Sure, we can kill off any calls that come from a known bad set of IP addresses (a standard black listing approach as used by many anti-spam engines). And we can let through any call that comes through from a known, trusted IP address (again, white listing, as used by many Spam engines). So, we manage to kill off or let through probably 20% of our calls, but what happens to the other 80%?

As soon as we start to take an active interest in the call itself, we introduce a delay. Telephony of any sort is synchronous, and for those of us old enough to remember the joys of transatlantic telephony in the 1960s, that quarter-second delay in conversations made your head reel.

The problem for Spit engines will be that all the tricks that the spammers have learnt from e-mail spam will be magnified here. It took spammers a while to realise that having a static IP address meant that the spam was cut off fairly rapidly by putting the IP address on a black list.

Now the majority of IP addresses used by spammers are either live only for 15 minutes or less and then dumped, or are completely spoofed randomly.

The farming of e-mail addresses that used to be so simple through just looking at [websites](#) for the "@" sign moved through to common name brute force methods of [john.smith@knowncompany.com](mailto:john.smith@knowncompany.com) – and we can expect brute force methods of IP sweeping to be used to identify IP telephony devices and target them in this way.

But to what end would anyone want to Spit, anyway? There is the slight chance that a virus could be written that could make the most out of the minimal intelligence built in to the phones. There is the use of mass cold calling, backed up either by cheap call centres or by recorded messages to sell holidays, time share or whatever.

However, the biggest one could well be the voice over IP denial of service attack – flooding a company's telephone service with essentially free

calls from automated IP autodiallers running at thousands of calls a minute such that no incoming or outgoing calls are possible.

So, when you are looking at your new VoIP installation, you may need to have a set of policies in place. Which handsets will have completely open usage, with only those IP addresses that are known to be Spite sources blacklisted, which handsets will have a broader block of IP addresses blocked, and which ones will only have access in or out to telephone numbers and IP addresses that are in a white list?

This can minimise your risk, and should any of the open phones start to be attacked, that phone can rapidly have a new IP address allocated so that the Spite engines would have to find it again.

Talk to the supplier and find out what they can do to help. Do they run their own white and black lists that you can utilise to get up and running rapidly? Do they have denial of service protection, so that the system can throttle down the number of incoming calls from dubious environments and still let those from known environments through? Does the VoIP system integrate into existing management systems so that you can utilise existing tooling to identify patterns of irregular usage?

VoIP has so much going for it, but runs the risk of being ruined by a mixture of reality and perception. Many systems are implemented as unmanaged systems, resulting in poor voice quality.

There is a perception that VoIP is insecure, but no one seems worried that the past 100 years of telephony has meant that anyone with a couple of crocodile clips can listen in to conversations, and that corporate VoIP is relatively easily secured.

However, Spite to me is the biggest risk – if companies find that they are bombarded with useless calls that cost the perpetrator very little but cost the company a lot in time, in resources and in capability, we may yet see a backlash against VoIP.

However, I believe that suppliers will be able to come up with workable systems that will be able to deal with more than 90% of Spite – but it is probably worth engaging in discussions with them now, rather than later.

## About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation’s environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca’s mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca’s clients include Oracle, Microsoft, IBM, Dell, T-Mobile, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca’s work and the services it offers can be found at  
<http://www.quocirca.com>