More from Jamie de Guerre, CTO of Cloudmark. All of the text below is Mr de Guerre’s own material with minor edits.

* * *

What do you see as the most promising new technologies coming down out of your research and development labs for the next stage of the fight against spam?

There are many innovations to choose from, many of which are back-end changes that are not visible to the public. Cloudmark also has several new products and services coming out this year, which are yet to be announced. However, the one I’m personally most excited about is Cloudmark ActiveFilter. The core battle between spammers and anti-spam vendors comes down to a race against time. Spammers are trying to get as many of their messages through as possible before the anti-spam vendors discover their messages to be spam. Essentially, ActiveFilter changes the game on spammers and takes the speed battle away.

Of the spam that Cloudmark misses, we typically only miss it by seconds or minutes (usually seconds). However, the majority of the time, that message is delivered to a user’s mailbox when the user is either not logged into their e-mail or is not reading their e-mail at that exact moment. If we were still able to filter the message within seconds once we discovered it as spam, the user would never have to see the message or know that it was initially missed!

What prevented this from happening in the past were performance considerations. In general, the mail-store server is an extremely loaded system in a customer environment, whether it is a Microsoft Exchange server or a large-scale server used by a service provider to host millions of mailboxes. Attempting to re-scan every message on the mail store every couple of minutes, or worse yet every few seconds, is nowhere near possible—it would quickly overload the system and degrade users’ ability to access their legitimate e-mail.

The innovation with ActiveFilter is that we are able to filter these messages after they arrive without needing any re-scanning and without any significant load on the mail store. We track a small piece of information about each message delivered to the mail store inside the ActiveFilter system, along with the fingerprints generated for the message. If we later discover one of those fingerprints to be spam, then, and only then, do we contact the mail store to take action on that particular message. In the case of a business deployment, such as with Microsoft Exchange, we would then change the color of the message in the user’s inbox and enable them to go to a “search folder” to see all of the spam messages that were detected after initial arrival and delete them. In the case of a service provider, we would check to see if the user had already logged into their e-mail since the arrival of the message; if they have not, we take action on the message with their default policy, such as to move it to a spam folder.

By taking the speed advantage away from spammers, I think we will be able to improve spam-filtering accuracy drastically; reaching the point that accuracy starts to approach 100%.
prospect is very exciting to me.

* * *

Jamie de Guerre started as a core member of the design team writing the first design specifications for Cloudmark Server Edition and multiple versions of Cloudmark Authority. As CTO, Jamie is responsible for Cloudmark’s technical strategy and roadmap. Additionally, Jamie manages Cloudmark’s Technology Services, Sales Engineering, Product Management and ISP Support teams, ensuring a tight bridge between customers and internal technical development. You may write to him with your comments.<mailto:jamie@cloudmark.com>

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2009 Jamie de Guerre & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.