The sys admin's daily grind: SpamAssassin 3.3

PHISHERMAN'S END

SpamAssassin is the backbone of countless anti-spam strategies. Its maintainers are cautious people and have just released the last major version since 2007. It's definitely worthwhile. **BY CHARLY KÜHNAST**

```
File  Edit  View  Terminal  Help
root@salami:/usr/local/Mail-SpamAssassin-3.3.0# ./sa-update --channelfile update-channels.txt
--verbose

Update available for channel saupdates.openprotect.com
Update available for channel 70_sare_stocks.cf.sare.sa-update.dostech.net
Update available for channel 70_sare_adult.cf.sare.sa-update.dostech.net
Update available for channel 70_sare_spoof.cf.sare.sa-update.dostech.net
Update available for channel 70_sare_bayes_poison_nxm.cf.sare.sa-update.dostech.net
Update available for channel 70_sare_genlsubj_x30.cf.sare.sa-update.dostech.net
Update available for channel 70_sare_oem.cf.sare.sa-update.dostech.net
Update available for channel 70_sare_random.cf.sare.sa-update.dostech.net
Update available for channel 70_sare_specific.cf.sare.sa-update.dostech.net
Update available for channel 70_zmi_german.cf.zmi.sa-update.dostech.net
Update available for channel 88_fvgt_bayes_poison.cf.sare.sa-update.dostech.net
Update available for channel 88_fvgt_tripwire.cf.sare.sa-update.dostech.net
Update available for channel 88_fvgt_rawbody.cf.sare.sa-update.dostech.net
Update available for channel 88_fvgt_subject.cf.sare.sa-update.dostech.net
Update available for channel chickenpox.cf.sare.sa-update.dostech.net
Update was available, and was downloaded and installed successfully
```

Figure 1: The --verbose parameter is new, but otherwise SpamAssassin 3.3.0 feels pretty familiar at first glance.

About a year ago, I wrote about SpamAssassin's own update function, SA-Update [1]. It keeps the rules that SpamAssassin [2] includes up to date and can integrate and update rules from third-party sources.

The detection rate my spam filters achieve depends to a great extent on these sources. I currently use the sources in Listing 1; line 1 provides the default ruleset.

The development team has just taken the next logical step and now provides SpamAssassin 3.3.0 without a standard ruleset. After completing the installation, you have to call *sa-update*. Alternatively, the distribution makers provide the rules themselves as a continually updated package. Or, you can create a cron job for *sa-update*. This forces those SpamAssassin users who are too lazy to update to protect themselves with the current ruleset.

Pleasant Surprise

SA-Update itself is fairly conservative; only the *--verbose* switch is new (see Figure 1). Originally, I considered the replacement of the previous DomainKeys plugin with a new Mail::DKIM in the new 3.3.0 version to be fairly inconsequential, but this is not true. Mail::DKIM supports Author Domain Signing Practices (ADSP). Behind this cryptic moniker lurks a potentially lethal weapon against phishing. DKIM gives you an easy approach to discovering whether the sender of an email message really is the person he claims to be.

But what if an unsigned email message arrives from the same domain? Does this mean it is a fake? Probably not, the sender could be a road warrior, and thus forced to use another, non-DKIM mail gateway. The ADSP DKIM extension makes it possible to store notes on signature behavior, or "Signing Practices" if you prefer, directly in the corresponding DNS record. If you find the key word *discardable*, this means: Dear Receiver, we sign all outgoing mail. If you received an unsigned message, we would advise you to ditch it.

If ADSP can establish itself with typical phishing-prone senders like banks, or online shopping centers, life is going to become hard for phishers. At last! ■

Listing 1: Additional Sources

```
01 updates.spamassassin.org
02 saupdates.openprotect.com
03 70_sare_stocks.cf.sare.sa-update.
   dostech.net
04 70_sare_adult.cf.sare.sa-update.
   dostech.net
05 70_sare_spoof.cf.sare.sa-update.
   dostech.net
06 70_sare_bayes_poison_nxm.cf.sare.
   sa-update.dostech.net
07 70_sare_genlsubj_x30.cf.sare.
   sa-update.dostech.net
08 70_sare_oem.cf.sare.sa-update.
   dostech.net
09 70_sare_random.cf.sare.sa-update.
   dostech.net
10 70_sare_specific.cf.sare.sa-update.
   dostech.net
11 70_zmi_german.cf.zmi.sa-update.
   dostech.net
12 88_FVGT_Bayes_Poison.cf.sare.
   sa-update.dostech.net
13 88_FVGT_Tripwire.cf.sare.sa-update.
   dostech.net
14 88_FVGT_rawbody.cf.sare.sa-update.
   dostech.net
15 88_FVGT_subject.cf.sare.sa-update.
   dostech.net
16 chickenpox.cf.sare.sa-update.
   dostech.net
```


INFO

[1] "New Order" by Charly Kühnast, *Linux Magazine*, March 2009, pg. 63, *http://www.linuxpromagazine.com/Issues/2009/100/NEW-ORDER*

[2] SpamAssassin: *http://spamassassin.apache.org*