README

July 6, 2003

Contents

1 What is this software?

smm is a anti-spam, mail-shaper, delete-on-server software thought for users who have a slow dialup connection and are sick and tired of downloading 1MB a day of spam and Win32-worm-attached messages. Since now it supports only pop3 accounts, and smtp accounts for complaining.

2 Why this software exists?

There are some other delete-on-server mail-filter programs, like mailfilter, but I've not found one with all these functions:

- portable (it runs natively on Linux and Windows)
- complex rules with logic operators (and,or,...)
- extended regular expressions match
- rules can use the message size (beware of large executable files)
- black list check for spammers
- interactive mode (to test and improve your rules)
- batch mode (if you trust your rules)
- UIDL database (if you use the "keep messages on server" pop3 feature)
- APOP (secure pop3 authentication)
- plugin architecture(other mail filters/mail protocols can be easily added)
- high configurable bandwidth usage (you can choose how many lines/bytes you want to download and check of each message)
- bounce message (simulate your mailbox is unavailable)
- multithreaded download (avoids slow DNS servers and slow pop3 servers)

Recently (on 5 February 2003) I discovered mailwasher, that is a closed-source software that says : "I'm freeware and spyware free". Superficially smm can be mistaken for an open-source clone of mailwasher. I've not taken any ideas from it and smm has been developed without knowing the existence of mailwasher.

3 Plugins

Since version 1.4 smm was a monolithic application. The I decided to implement a plugin interface to make easier to expand smm functionalities. Smm is bundled with all currently available plugins. You must activate them before run smm for the first time. Click on plugins ▷ available to mark some of them as active and to configure them. There are plugins for fetching mail, checking mail, other stuffs. You should activate at least one plugin for fetching mail and one for checking it. You must restart smm to make configuration changes work. See the developer manual for more info about the plugin interface.

4 How it works?

Syntax: smm [- -batch | -b] [–semi-batch | -s] [–help | -h] [–version | -v] [-c <dir> | –config-dir <dir>]

smm runs in interactive (default), batch, and semi-batch mode. The batch mode acts as you click connect and then disconnect and quit in the interactive mode. Semi-batch works as batch mode, but a popup windows is displayed at the end of the filtering process. To start *smm* in batch mode use the –batch option, –semi-batch is for semi-batch mode, –help is for a short help screen and –version is for license and version details. Interactive mode is useful for testing your rules and configuring properly smm, while batch mode is recommended when your rules are clever enough. If you want to use an alternative (than your home ~/) directory for config files, you can use -c or –config-dir. For example to use "smm -c ." creates ".smm" in the working directory and uses the created files instead of looking in your home.

4.1 Short description of an interactive mode session.

1. Click the connect button.
2. Now you have the list of mails on your servers. You can see the fist few lines clicking on them. *smm* checks each mail with your rules and puts a green or red semaphore near each message. Red messages will be deleted on the server, green will be untouched . Now you can change the semaphores color clicking on it or using the keep and the delete buttons.
3. Click the disconnect button and unwanted mails will be deleted from servers. Now you can download your messages with your favorite client, or fetch them with fetchmail.

If you are testing you rules (plugins configuration) you should check the log window to see the configuration file parser output, and the result of applied rules.

5 Bouncing

In interactive mode you can select one or more messages and click bounce. This will open a window for sending a mail to the spammer/guy-with-infected-win32-pc. Remember that some worms hide the real identity of the sender, so look carefully to the header of the received message. smm can simulate a permanent failure in the mail transport system as if your mailbox is full or inexistent. In the option window you can choose the default bounce message. I think bouncing is illegal, since you send a mail as the MAILER-DAEMON of you provider, saying that a mailbox is unavailable or similar. Maybe some spammers will be confused and will delete your name if they received a bounced mail. If you want to see what this feature does, send a mail to yourself and bounce it back. You will receive a standard mail transport agent report message about a failure in the delivery process.
Version 0.19 adds the “auto bounce red flagged messages on disconnect” . In the option window you can activate this option. This option works only in interactive mode and automatically opens the bounce window for messages with the red semaphore when you click the diconnect button. This option is not available in batch and semibatch mode (if you want me to change this behaviour you must convince me that this will not make smm a software that tryes to kill spam generating more spam. back-spam is not the solution).

6 The configuration files

smtp accounts and pop3 accounts have a nice gui based configurator. You don’t need to edit smmrc and pop3rc manually. Other plugins don’t have a so user friendly interface, but can be configured from the interactive mode too.You should be the only user who has read permission on configuration files, since they contain plain text passwords.

In ~/.smm/ (Unix) or in the program directory (Win32) there are some other files. In the logs directory you can find smmlog and pop3netlog. The first is the system persistent log, while the second is a dump of the pop3 plugin log window (You must have write access to these files).

7 Plugins

To configure and activate plugins click Plugins▷ Available.

7.1 Pop3

The pop3 plugin is able to download mails from the pop3 server. You must configure properly this plugin setting up your accounts. The fields host, port, username and password are really common and you can copy them from your mail client as they are. The strange field is login. Here you can choose the authentication method. CLEAN means to send password in clear text. APOP sends your password in crypted mode, but

is not supported from all pop3 servers. FALLBACK tries APOP and if it fail it tries CLEAN. I experienced that some stupid pop3 server that don't support APOP will wait one life before saying "I don't know what APOP is!". CLEAN should be used also with these really clever servers.

7.1.1 UIDL support

If your pop3 client is configured to "keep messages on server", you should activate the UIDL support in Settings ▷ Pop3Accounts. If UIDL support is on, smm will not check old mail. This makes smm faster, because It will not download the same message twice. If you want to inspect again your mailbox (maybe you changed some rules and want to test them on a message that has already been analyzed) use the Settings ▷ Pop3Accounts ▷ CleanUIDLdatabase button.

7.1.2 NOOP delay

Usually pop3 servers implements a feature called *automatic disconnection*. If an open connection has no activity for a while the connection is automatically terminated. This is a little problem for smm. When you choose in interactive mode which message to delete, the connections are still open, but there is no activity on them. To avoid this problem smm sends a NOOP message on each connection every NOOPDELAY seconds to keep the connection alive. rfc1939 says that the right timeout for disconnection should be 10 minutes, but in my experience I've understood that the majority of pop3 servers usually close an inactive connection after one minute or less. You can choose the delay between two NOOP messages in the pop3 config window. I hope 20 seconds is enough for all pop3 servers.

7.2 Yahoopops

This is a simple plugin that adds a dropdown menu to start YahooPops with one click from smm. On Unix you must have the yahoopops executable in your path, while on windows you must configure this plugin setting properly the path in which yahoopops is installed.

7.3 RblCheck

This plugin uses blacklists for discovering if a message is sent by a spammer. If you active this plugin remember to configure it and select one or more blacklists. You can add an arbitrary number of blacklists. A message will be deleted only if the major number of active blacklists will say that the sender of the message is a spammer.

7.4 Inspector

This is probably the most powerful plugin, but is not trivial to configure it. It makes regular expressions based checks. If you don't know what regular expressions are you should search the web. The configuration file is divided in 3 sections.

POLICY SECTION here you can choose if a doubt rule should be treated as a delete rule. This is useful for debugging your rules looking at the Inspector log window.

NAMES SECTION here you can specify some "names". You can define a SIZE name like "SIZE [wormsize] = 100K to 500K ;". In the next section using wormsize you will refer to a size of 100-500K. The other king of name is NAMELIST. A namelist is a sequence of regular expressions. An example is "NAMELIST [wormtitles] = [A.*powful.*tool] [A.*game] ;". Now wormtitles is a list of regexp that can be used in the next section.

RULES SECTION You can define 3 types of rules: DOUBT DENY ALLOW. If a message is positive to an ALLOW rule it is considered a good message. If a message is positive to a DENY rule it will be deleted. The DOUBT policy is specified in the first section. A rule is something like "DENY [worms] = SIZE is_in [wormsize] ;". This rule has a name "warms" and will delete each message

which size is in the “wormsize” range. This means that if the message is from 100K o 500K smm will delete it. This is a stupid example to introduce the rules structure. A rule starts with one rule type keyword: DOUBT DENY ALLOW. Than you must specify the name that is useful only for debugging. Than the rule is something like: emailpart predicate name. emailpart is one of SUBJECT SIZE SENDER HEAD BODY. SIZE can be used only with a SIZE name (see the first example of the second section). I think that some example will make this simple.
DOUBT [firstrule] = SUBJECT is_in [wormtitles] ; this rule is positive if the subject of the message matches one or more of the regular expressions defined in wormtitles. For example if the title is “A really powful and nice tool” the message will be doubted.
DENY [secondrule] = (SIZE is_in [wormsize]) and (SUBJECT is_in [wormtitles]) ; is a more clever rule. The message is deleted only if the size is between 100K and 500K and if the subject matches the wormtitles list. The configuration file of Inspector is well commented and there are some prebuilt useful rules.

7.5 Spamassassin

7.5.1 Introduction

smm can use spamassassin engine on partially downloaded mails. I think this is a great feature, since the standard spamassassin usage is on fully downloaded emails, while users with a slow dialup connection would like to optimize bandwidth usage.

7.5.2 The problem

Since spamasassin thinks that is working with a complete email, it gives some penalities to uncomplete messages, for example a message with a truncated attachment has a 0.2 penality. But a good message, partially downloaded with smm, will probably have something truncated.

7.5.3 The solution

You only need to add this line to your ~/.spamassassin/user_prefs (you can change this file from the spamassassin plugin configuration window)

```
score MIME_MISSING_BOUNDARY 0
```

7.5.4 Considerations

I’m not a spamassassin guru, so there may be other useless checks to remove.

8 Security

I know that there are at least 4 ways to login on a pop3 server. I’ve implemented the simple but insecure USER-PASS login and the widely used APOP-md5. You can choose between secure and insecure connection for each server. Remember to protect ~/.smm/ from reading to others. *smmrc* contains your passwords and *smmlog* the header of deleted messages.

9 Download policy

Since version 0.16 smm support a more complex download policy called “shaped”. The classic policy was: “download always N lines of each message”. The shaped policy is more complex but allows you to optimize the bandwidth usage. A “shape” is a size range and an amount of lines/percentage to download. For example a shape is “if the message size is greater-equal than 100 bytes and smaller than 3000 bytes download 18 lines”. You can add an arbitrary number of shapes in the options window, but remember that they may not overlap. If you choose to download 0 lines, only the header is downloaded. If you choose

to skip the message it will be skipped by smm, and you will not see the message in the list. If you choose the % amount, the number of lines to download is calculated dynamically using the message size and the medium line length you have chosen in the option window.

10 Why multi-thread?

Multi-threaded mail download speeds up the download process since it connects simultaneously to all your pop3 accounts. This avoids big network latencies, like hostname resolution via DNS or connection to an hi-loaded server. Under Linux this approach makes possible to redraw the guy during the download process, and this cuts out the annoying guy freeze. Under windows this is not possible because of a "conflict" between gtk and threads, so the GUY may freeze, but the download speed is increased.

11 Why LyX and not LaTeX?

Simple. When I started writing this I had no knowledge of LaTeX.

12 Testing

I've tested smm with qpopper by QUALCOMM using a loopback connection and some people I thank have reported me bugs I've tried to solve :)