Third Secure List Server bi-monthly project report

Joost van Baal <joostvb@ad1810.com>

January 26, 2009

Introduction

As agreed upon in the June 13, 2008 document "Memorandum of Understanding Secure List Server Project", this report documents work done by the author for the Secure List Server project (http://non-gnu.uvt.nl/mailman-pgp-smime/), as funded by the NLnet Foundation. It also lists the current plans for the project.

This document is a follow-up to the Second Secure List Server bi-monthly project report, as sent to Valer Mischenko on November 1, 2008.

1 Completed tasks

Here's a condensed overview of the progress made thus far.

Task	Planned	Delivered
(Start project)	08-07-01	08-06-24
(Milestone 1)	08-08-15	08-08-09
Publish first project report	08-09-01	08-08-31
Bug: Implement test suite	08-10-15	08-10-30
Publish second project report	08-11-01	08-11-01
Bug: Enforce confidentiality	08-11-15	09-01-02
Bug: Better user interface	08-12-15	09-01-02
(Milestone 2)	08-12-15	09-01-06
Publish third project report	09-01-01	09-01-26

See the first and second reports for details on the tasks completed for Milestone 1, as well as for details about the test suite.

The 2 Bug-tasks ("Enforce confidentiality" and "Better user interface") are found by Security Auditor Guus Sliepen and published in "Security Audit of the Secure List Server, Part I", August 1, 2008.

About "Enforce confidentiality", Guus wrote (paraphrased):

"If an encrypted message sent to a list is for some reason automatically discarded, the auto-discard notification is sent to the list administrator, but it contains an decrypted copy of the original message. This breaches the confidentiality of the original message. An encrypted message should either be forwarded encrypted or not at all.

"Emails with a valid signature of a known subscriber are accepted regardless of whether the address in the From header matches one of the email addresses associated with the key. Since the original signature is removed before the mail is sent to the other subscribers, this allows one subscriber to impersonate another subscriber or even an outsider.

"When a list is set up for integrity and/or confidentiality, these aspects should *always* be enforced. This means that an encrypted message sent to a list *never* leaves SLS unencrypted. It is also strongly recommended to try to keep the original signature of messages sent to a list, but in case of OpenPGP this might not be possible without support from the GnuPG developers."

About "Better user interface", Guus wrote (paraphrased):

"The list administrator interface is not very clear. For example, one of the options is: "Should messages be GPG signed? Yes means: hold for approval. (No, Yes, Force)". It is unclear from just this question what the difference between Yes and Force is. Will Force add a signature if there is none present, or twist the subscriber's arm until he does? If I answer Yes, does that mean that signed messaged are held for approval? It takes a while before one guesses the true meaning of the choices. It is better to rephrase the question to "Allow unsigned messages? (Yes, Hold, No)", or to elaborate the choices in the original question: "No, Yes (hold unsigned), Force (drop unsigned)". The sames goes for all the other three-choice option.

"Although one can easily upload OpenPGP keys via the website, there is no way to upload an S/MIME list key. With the current patch, the list administrator somehow has to put the S/MIME list key in /var/lib/mailman on server running SLS.

"Once someone is subscribed to the list (possibly only after getting permission from the list administrator), he can log in to the list manager web interface with just a password and change his settings. This also allows him to change his public key. Since a public key is a much stronger credential of someones identity than just an email address, and since it is much easier to guess a password than to crack a key, it should not be allowed to change the public key without explicit permission from the list administrator."

Some extra time was spent on keeping our code in sync with upstream by merging it, by upgrading our test environment and by releasing versions 2008-11-16, 2008-12-14 and 2009-01-02 of the patch, available from `http://non-gnu.uvt.nl/pub/mailman/`, announced on the GPG/SMIME mailman devel list at Sun, 16 Nov 2008 and later.

Feedback has been given to Brad Borevitz and Hanno Böck on the GPG/SMIME mailman devel list at Nov 3, 2008.

Work on task "Disseminate results", scheduled for completion at 09-03-01, has been started: A lightning talk request for fosdem has been submitted on 08-11-06 and got accepted, see `http://fosdem.org/2009/schedule/events/secure_list_server`. The fosdem conference (see `http://fosdem.org/`) will take place Saturday 7 and Sunday 8 February 2009 in Brussels.

Futhermore, a talk request for the Chaosseminar in Ulm has been submitted 08-11-24. The talk took place at 09-01-12, see `http://ulm.ccc.de/ChaosSeminar/2009/01_Mailman_PGP_SMIME`. The talk has been recorded on video, the recordings will get published 2009-02. About 17 Free Software developers (featuring Stefan Schlott, the original SLS-patch author) attended the talk, which started at 20:00. A lively discussion went on till 21:30.

Work on task "Write and publish documentation", scheduled for completion at 09-01-15, has been started: An article has been handed out to the Ulm talk audience, it's available from `http://non-gnu.uvt.nl/mailman-pgp-smime/pgp-smime/talk/`.

The talk was announced as:

"*About the project*

"The Secure List Server, mailman-pgp-smime, is an effort to add support for encryption and authentication to Mailman, the GNU mailing list software. This enhancement enables groups of people to safely cooperate and communicate using email. The patch includes support for both RFC 2633 (S/MIME) and RFC 2440 (OpenPGP) email messages.

"Work on this software was started by Stefan Schlott, in 2005 (or earlier). Development of the

patch currently is made possible by the NLnet foundation.

"A post to a secure list will be distributed only if the PGP (or S/MIME) signature on the post is from one of the list members. For sending encrypted email, a list member encrypts to the public key of the list. The post will be decrypted and re-encrypted to the public keys of all list members.

"The software is GPLv2 licensed. More information is available from `http://non-gnu.uvt.nl/mailman-pgp-smime`.

"*About the talk*

"The talk will start with a very short overview of the history of Mailman and the mailman-pgp-smime project. Some remarks will be made on how to install and configure the software, so that one can try it. Currently supported features will be mentioned, as well as an overview of development plans. One will learn how to contribute to the project; an overview of the revision control system used will be given. Some remarks on the future of the patch will be made: will it be shipped with Mailman itself?

"If you have used Mailman, both as a subscriber and as a list admin, and if you know what PGP and S/MIME are, you should definitely attend this talk.

"The talk will be given in English.

"*About the speaker*

Joost van Baal is a DJ since 1995. Debian developer since 2000. Working on Lire, LogReport's log analyzer, since 2000. Free software advocate since 2001. Hacking on Mailman since 2005. Pugilist since 2007. Owner of ad 1810 since 2008. Joost works and lives in Eindhoven, The Netherlands. See `http://mdcc.cx/`."

2 Planned tasks

As requested by Valer Mischenko on Tue, 18 Nov 2008, the planning has been adjusted. "Try get SLS shipped w/ distros" is postponed from 09-03-01; "Fifth and final project report" and "(Milestone 4)" are postponed from 09-04-01. Current plans are:

Task	Planned
Write and publish documentation	09-01-15
Create a package of SLS	09-03-01
Publish fourth project report	09-03-01
Disseminate results	09-03-01
(Milestone 3)	09-03-01
Act upon auditors final report	09-04-01
Try get SLS shipped w/ distros	09-04-15
Fifth and final project report	09-04-15
(Milestone 4)	09-04-15

I'll also contact Mailman developer Barry Warsaw and ask him to perform his review he has offered via the Mailman Developers list.

The documentation will be written for users, for list admins, for site admins, as well as for developers.

Both a Debian and an RPM package for SLS will get build and published.

Currently, Guus Sliepen is working on his final security audit report.

In order to get SLS shipped with Free Software operating system distibutions, maintainers of

Mailman packages for e.g. GNU/Linux distributions (and the Sabayon and Smallsister projects) will get asked (and offered help) to include the patch. The author will work with the Debian Mailman package maintainer to try to get the patched Mailman shipped with Debian and Ubuntu, as discussed in a private conversation with the maintainer, Tilburg, 2008-06-06. The decision on wether or not to include this patch is under control of the package maintainer (not the patch author).