## Secure email with Thunderbird and Enigmail

# BIRD SECURITY

Thunderbird offers several options for secure email, and the GnuPG-based Enigmail encryption add-on provides an additional layer of protection.

**BY PATRICK BRUNSCHWIG, OLAV SEYFARTH**

The small-footprint, user-friendly Thunderbird email client is rapidly gaining ground with the Internet community. Most Linux distributions include Thunderbird [1] by default. The Mozilla developers have ready-to-run versions for most current systems on their website. Debian does not have an official package for the current version, but test versions are available from the maintainer's repository [2].

With the recent Thunderbird prerelease version 0.9, the bird is almost ready for flight with an impressive collection of convenient security features. In this article, you'll learn some of the finer points of Thunderbird security.

## Authentication

Thunderbird supports POP, IMAP, and SMTP for email, as well as NNTP and SMTP for News and LDAP for addressbooks. These services typically require authentication. In the simplest case, the client will want to transmit login and user payload data in the clear, opening up an attack vector for eavesdroppers. Thunderbird gives users a number of secure authentication approaches to combat this.

Challenge-Response approaches transfer a secret (such as a password for example) as a temporary hash. This approach relies on the server being able to support it, of course. Thunderbird will attempt to detect the server's capabilities, but success is not guaranteed. Although DIGEST-MD5 and CRAM-MD5 are auto-negotiated for SMTP nodes, you will need to enable CRAM-MD5 for POP and IMAP accounts using *Enable secure authentication* in the server options for your mail account.

## Traffic

Unfortunately, Challenge-Response techniques do not provide any protection against man in the middle attacks. For additional security and privacy, you can encrypt the traffic between client and server using the Transport Layer Security (TLS) protocol. TLS (a successor to the SSL protocol) encrypts any communication between the client and the server. Thunderbird only supports TLS for SMTP.

When you set up a new account using the Account Manager, the connection will be insecure at first. Before connecting to the mail server, open the *Tools | Account Settings* dialog box, where you can set up individual protocol settings. In *Account name | Server settings*, select *Use secure connection (SSL)* (Figure 1). Thunderbird will configure the port automatically. For *Use secure authentication*, you should preferably select *CRAM-MD5*.

For *Outgoing server (SMTP)* you will want to tell Thunderbird to use your user name and password, along with a secure connection. In this case, *TLS* means enabling Start TLS; the port for SSL is configured automatically. In *Tools | Settings | Compose* you can also set LDAP servers to SSL connections in *Address autocompletion*.

## Encrypting Passwords

Security conscious users with multiple email providers will want to select a dif-

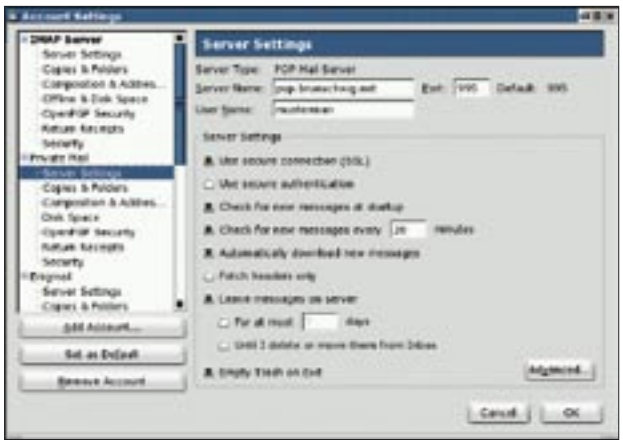

**Figure 1: The Thunderbird Server Settings dialog box has an option for configuring a secure connection.**

ferent password for each provider. As it can become difficult to remember all these passwords, and as it is definitely annoying to have to type them repeatedly, Thunderbird allows users to store passwords.

In the default setting, Thunderbird will Base64 encode your passwords; that is, it will not encrypt them and will store them below your user profile in a file with a random name and the *.s* extension. This approach to security is a compromise that you might be willing to accept if you are the only user to access the system. The software cryptography module based on the Mozilla Network Security Services (NSS) provides users with better security by encrypting stored passwords.

There are different opinions on password storage, but Thunderbird's password encryption feature seems to be a workable compromise. If you require Thunderbird to store email addresses in a password-protected LDAP directory, you will have no alternative but to store your passwords, as each new email opens a new connection to the LDAP directory, which would mean retyping your password.

To encrypt existing and future passwords, you need to enable *Use a master password to encrypt stored passwords* below *Tools* | *Preferences* | *Advanced* | *Saved Passwords* | *Master Password* and then set your master password by selecting *Change password*. As this password will need to protect all your other passwords, and your own X.509 certificates, make sure it is really robust. To create a secure password, ensure that your password is long enough, contains small and capital letters, numbers, and special characters.

## Signed and Sealed

After securely authenticating against your service provider's mail server, you will probably want to encrypt any messages stored on this server. Today's worm attacks steal user names and dispatch email messages using these names.

There are two mutually incompatible standards, S/MIME and OpenPGP, that give you this kind of security. Thunderbird supports both, assuming you have installed the Enigmail [4] add-on, however; keep in mind that neither S/MIME nor Open PGP provide a complete security solution. As described earlier in this article, you'll also need to take steps to protect the user data and the login process.

## Enigmatic Machine

The Enigmail OpenPGP add-on was developed as a sample application for interprocess communication. In 2001, Mozilla developer Ramalingam Saravana developed a library for opening and managing pipes. As Mozilla did not have OpenPGP encryption at the time, he coded a small add-on for test purposes. The add-on passes and encrypts web mail to GnuPG and displays the decrypted text in the browser (Figure 2). This was the start of a major add-on for the Mozilla email client and later for Thunderbird.

Enigmail does not automatically import public keys (although you can set up GnuPG to do so by specifying *keyserver-options auto-key-retrieve*), however, it can search public key servers for matching keys when you send a message. Many Linux distributions integrate Enigmail support with Thunderbird, or they at least provide a separate package, for example *mozilla-thunderbird-enigmail* for Debian.

If you are using the plain vanilla version from the Thunderbird web site, you will need to install Enigmail via the extension manager. Make sure the Enigmail version matches your version of Thunderbird, as Thunderbird may crash otherwise. Additionally, Enigmail and Thunderbird need to speak the same language.

After the install, first check if Enigmail is working correctly and finds GnuPG. To do so, open the *Enigmail* | *About Enigmail* menu. The first time you do so,

### Certificate Management

In most cases, you will want to use a SSL-protected connection in your web browser to pick up your certificate from the CA. Integrated packages such as the Mozilla suite allow the browser and mail program to use the same certificate store. Thunderbird has its own store, and even if you use the Firefox browser parallel to Thunderbird, you will still need to download the certificate with your browser, store it in a PKCS-#12 file, and import the file into Thunderbird.

Certificate management is located in *Tools* | *Preferences* | *Advanced* | *Certificates* | *Manage Certificates*. There are tabs for your own secret key-protected certificates, certificates from other users, web sites (SSL/TLS certificates from mail and new servers) and CA certificates (which you have added or which were supplied by default).

In some cases it makes sense to have two certificates per user: one that is known within your organization for encryption purposes. This would allow a program running on your gateway to decrypt mail messages and check them for malware. Another certificate would belong to the user and be used for signing purposes. After importing your own certificates, select a certificate for signing outgoing messages and another certificate for encryption and decryption purposes below *Security* in your account settings.

To encrypt a message, you will need the recipient's certificate. If this can't be obtained from your PKI, you will need to ask the recipient to send it to you. It is perfectly acceptable for the recipient to send you a signed email message by reply mail, as any certificates the message contains will be imported automatically. As an alternative, you can run a search against a meta keyserver or the certification authority to locate the certificate; Thunderbird itself does not have an integrated feature that does this for you.

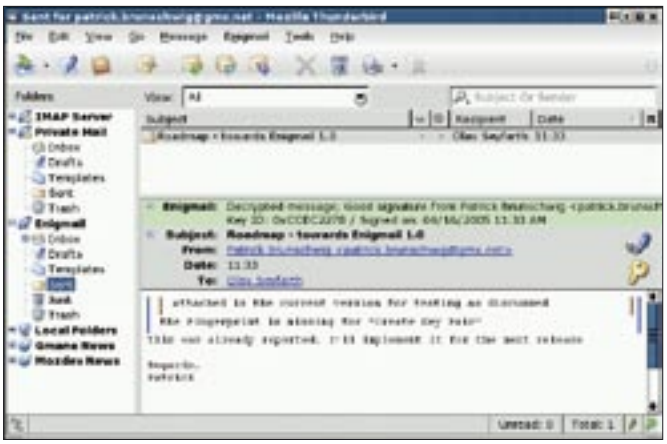

**Figure 2: Enigmail encrypts and decrypts mail messages in Thunderbird.**

you are asked if you want to configure Enigmail. You can say no at this stage and return to configure Enigmail some time later.

In the window that pops up, the third line should have a message telling you: *Using gpg excecutable path to encrypt and decrypt*. If you see an error message at this point, this means that Enigmail has either failed to find GnuPG, or that the Enigmail version you have installed is not compatible with Thunderbird.

If you do not have an OpenPGP key, you can generate the key using the key management feature *Key | Generate key*. To send OpenPGP-signed or encrypted messages, you need to set up Enigmail for each account. This tells Enigmail to add an extra *OpenPGP Security* tab for each account. This is where you select the keys to use, and specify defaults for encryption and message signing. Although it is more convenient to allow the program to select the key automatically based on the sender's email address, this approach is inherently insecure if multiple keys are mapped to the same address.

OpenPGP supports two encoding standards: Inline-PGP and PGP/MIME. Inline-PGP only encrypts the message body, but requires the user to encrypt attachments separately and to attach the encrypted files to the message. Also, Inline-PGP does not support HTML messages with formatted texts, and extended character sets such as Chinese can cause problems. PGP/MIME encrypts the message including any attachments and formatting en bloc and thus resolves all of these issues – unfortunately, not all PGP-aware email clients support PGP/MIME.

Enigmail has a number of options for controlling GnuPG and Thunderbird below *Enigmail | Preferences*. The defaults make sense for most users, but to optimize use of Enigmail, you may still prefer to change a few Thunderbird defaults. To make this easier, the Enigmail extension unhides a few Thunderbird options that are normally hidden. See the box titled "Enigmail Options" for some critical settings.

## Keeping to the Rules

Enigmail has a rule editor that allows you to define settings for signing, encrypting, and applying PGP/MIME and key IDs per recipient or group of recipients (Figure 3). The editor allows you to set preferences for the selected email address. Enigmail not only supports rules for individual users, but also for groups of users, such as all the addresses in your company.

The integrated help function has detailed information on per-recipient rules. Thunderbird automatically applies these rules when sending messages, so it makes sense to leave the Enigmail security prompt enabled. This gives you a reminder, just in case you attempt to send an unencrypted message.

Thunderbird has everything that the security conscious user could wish for, although simple application of modern encryption technologies is still a distant goal – as some of the pitfalls we have discussed would suggest. ■

**Figure 3: The Recipient Settings dialog lets you configure OpenPGP rules for specific recipients.**

## Enigmail Options

Enabling the *Enigmail | Preferences | Sending | Allow flowed text* tells Thunderbird to break lines in a message into multiple lines if the lines are longer than permitted. The mailer adds the quote character ">" in the continued lines. Unfortunately, this breaks the signature that Enigmail creates for the original message. When replying to messages, Enigmail thus replaces ">" at the start of a line with "|", thus preventing Thunderbird from changing the line. But it still makes more sense to disable the flowed text option.

To decrypt PGP/MIME encrypted messages stored on IMAP servers, you will not be able to download individual MIME parts. Otherwise Enigmail does not get the complete message from Thunderbird and can't decrypt the message. The *Enigmail | Preferences | Advanced | Load MIME parts on demand* option allows you to change this behavior.

To decrypt Inline-PGP messages, you will need to disable HTML rendering in messages through the *View | Message Body | Plain text* option.

Enigmail supports both Inline-PGP and PGP/MIME. If you are sending a message with attachments, you are asked whether you want to encrypt the attachments individually or use PGP/MIME to send the message. You can use the context menu to decrypt and open encrypted attachments in incoming messages. Enigmail can store different defaults for signing and encrypting messages based on the sender account information.

## INFO


[1] Thunderbird product page: *http://www.mozilla.org/products/thunderbird*

[2] Thunderbird and Enigmail Debian packages *people.debian.org/~asac/testing/*

[3] CVS snapshot: *http://ftp.mozilla.org/pub/mozilla.org/thunderbird/releases/0.9/thunderbird-0.9-source.tar.bz2*

[4] Enigmail: *http://enigmail.mozdev.org*