I2P-Bote

Secure Distributed Email

- HOME
- DOWNLOAD
- SCREENSHOTS
- USER GUIDE
- FAQ
- FORUM
- CONTACT

I2P-Bote is a plugin for I2P that allows users to send and receive emails while preserving privacy. It does not need a mail server because emails are stored in a distributed hash table. They are automatically encrypted and digitally signed, which ensures no one but the intended recipient can read the email, and third parties cannot forge them.

Latest version:

I2P-Bote 0.2.5 (Oct 4, 2010)

This program uses:

I2P The I2P Anonymous Network

More links:

- Deutsches Handbuch
- Latest I2P-Bote code checkins
- Freemail, a vaguely similar project

Features:

- Webmail interface
- One-click creation of email accounts (called email identities)
- Emails can be sent under a sender identity, or anonymously
- ElGamal and Elliptic Curve Encryption
- Encryption and signing is transparent, without the need to know about PGP
- Some say it's very cool

Planned Features:

- POP3 / SMTP
- Custom folders
- A distributed address directory
- Delivery confirmation
- Lots of small improvements

CSS: David Herreman

XHTML - CSS

I2P-Bote Manual

1. Introduction

I2P-Bote is an easy-to-use, highly anonymous secure e-mail application for I2P. It is a serverless, fully decentralized system that establishes/forms a peer-to-peer network built on top of state-of-the-art low latency anonymizing network I2P; adding to it an optional mixminion-like high-latency transport and thus avoiding the shortcomings of low-latency networks.

Therefore, I2P-Bote makes full use of the anonymity provided by I2P, plus it generates its own anonymity by adding another anonymizing layer (overlay network).

This concept of layered anonymity is what makes I2P-Bote so flexible:

You can configure it to be extremely anonymous and slow or less anonymous but faster/more efficient. In any event, I2P-Bote always provides a very good anonymity for both, sender and receiver, as well as end-to-end encryption*.

I2P-Bote offers the option to make your communications even more anonymous, by enabling the high-latency mail routes – at cost of performance, however. Users that want their anonymous e-mails to arrive as quickly as possible, will want to disable the mail routes and use 'direct' sending through I2P. It is guaranteed that you will never be less anonymous than the anonymity provided by standard I2P connections.

In order to achieve high usability, we have enabled it to be used with standard mail clients such as Thunderbird, Evolution or Kmail, without having to worry about what extra information these applications send in their headers. [YET TO BE IMPLEMENTED] Furthermore there is a web interface that lets you send and read e-mails or manage your settings and identities.

Current version is 0.2.5.

I2P-Bote is easy to use:

If you're not yet using I2P, just install I2P from http://www.i2p2.de and then install the I2P-Bote plugin as described in this manual. Otherwise simply read on!**

*Unless you send e-mails to or receive them from the regular internet, ALL emails – the mail body, attachments and the header except recipient's address (subject, date, time, sender address, ...) are automatically and transparently end-to-end encrypted. The recipient's address is only visible for the mail route's last node that stores the packets into the kad network, and the respective storing nodes, but they cannot read the mail's content nor who sent it nor who will fetch it.

**Of course you can also compile from source.

2. Howto

2.1. Installation

In order to install I2P-Bote, go to the bottom of the I2P Client Configuration page at

http://localhost:7657/configclients.jsp

and enter:

http://tjgidoycrw6s3guetge3kvrvynppqjmvqsosmtbmgqasa6vmsf6a.b32.i2p/i2pbote.xpi2p

(http://i2pbote.i2p/i2pbote.xpi2p might work, too, if you have i2pbote.i2p in your address book or a subscription)

in the “Plugin Installation Download Url” line, then hit “Install Plugin”.

Wait until your sidebar says plugin installed and started.

In order to update your I2P-Bote instance, click 'Update' under I2P-Bote on the I2P Client Configuration page at http://localhost:7657/configclients.jsp

2.2. Using I2P-Bote

On your router console http://127.0.0.1:7657/ click on 'SecureMail' on the upper left (in the sidebar). Now you are on I2P-Bote's web interface.

If you want to use I2P-Bote for yourself, you first need to create an identity.

After starting I2P-Bote (by default it is set to start automatically when your I2P router starts up) it takes a bit more than three minutes for everything to be up and running.

So have a look at 'Network Status' on the left. It should state 'Connected'.

2.2.1 Creating an Identity

Click on 'Identities' on the left, then hit the “New Identity” button.

Enter at least a 'Public Name' and hit 'Create'. That's all that's needed to create an identity.

The public name is the name you see for this identity (useful in case you have different identities for different sets of users you communicate with or different purposes) and it will be sent as “sender's name” to the mail's recipient. There is no need for Public Name to be unique.

(As you can choose any name here – anyone could call himself HungryHobo there – it is not suited to be used by the recipient for telling if two mails come from the same sender. This is why the name saved in the local addressbook (there can only by one name per destination key) is displayed, if there is any, and you will see a green mark in the “Loc” column, stating it is the locally known name. If there is no entry for a destination in local addressbook, the name specified by the sender will be displayed with a prefixed [UNK] in the mail clients). [POP3 NOT YET IMPLEMENTED]

You can also fill out the other fields, if you like.

Description – this field is kept locally. It's just for your convenience: If you want to add some additional information for yourself about that identity, you can enter it here.

Email Address – this field is not used yet.

Choose from one of the given encryption algorithms. If in doubt, stick to the defaults.

You click on the name of one of your identities and copy the long key displayed under 'Email Destination'. This is your I2P-Bote e-mail address. If you want anybody to be able to send you a bote mail, he need to be given this long key.

Now you can send and receive I2P-Bote mails.

But you should also have a look at your I2P-Bote settings and see if they fit your needs.

(You can also create various identities and assign different settings to each of them.)

2.2.2 Sending and Receiving E-Mails

You need to have the I2P-Bote e-mail destination key of the user you to whom you want to send a bote mail.

In order to send a message, click on 'New', choose your own sender identity or 'Anonymous' under “From” and enter the recipient's e-mail destination key or alternatively an address in the “To:” line.

Alternatively, you can hit the “Addr. Book” button right under this very line, in order to chose from e-mail dests stored locally in your address book: Mark the user(s) to which you want your mail to be sent and hit the “Add Recipients” button.)

You can add several recipients and change the 'To:' to 'CC:' or 'BCC:'.

The “+” button adds additional recipient lines.

Now write your bote mail and hit 'Send' for sending it, or 'Save' in order to store it as a draft into your 'drafts' folder or any user-defined folder. [not yet implemented]

Hitting “Send” will place your e-mail into the Outbox folder and you can go on using I2P-Bote, e.g. writing another e-mail, or simply do other things. I2P-Bote is now sending your e-mail. Once it is sent, it's automatically removed from Outbox and stored into your Sent folder. This means, your mail is entirely on the way to its destination (unless you have set a delay time, which is disabled by default).

In I2P-Bote e-mails are automatically signed (unless send without any sender identity).

You can also send e-mails without specifying *any* sender identity/destination/address, just select “Anonymous” in the scroll-down menu “From:”.

In the default settings I2P-Bote will automatically check for new mails, and all you need to do in order to see if you got e-mails is look into your Inbox (link 'Inbox' on the left).

You can force a manual check by clicking the 'Check Mail' button. This is a global checking, that tries to fetch new mails for all of your identities, except for those you have excluded from global checking. [not yet implemented]

The number of unread e-mails is shown in parenthesis next to the folder's name in the sidebar.

Click on “Inbox” to have a list of received e-mails displayed. You will see two columns with x's or green checks. Those show you if a mail contains a valid signature and is thus authentic (Sig) and if the sender's e-mail destination key is locally known, i.e. in your addressbook (Unkn/Loc). Hence, two green checks next to a mail entry mean that you already know that e-mail identity and that the mail is signed by that identity.

If you have a certain name in your address book and you get a mail from an identity with that name, yet Loc is *not* displaying a green check, then it is a *different* destination that sent and signed this mail; he simply has chosen the same name you have chosen for one of your contacts.

Is there a green check mark for “Sig”, then the mail is correctly signed by the sender and you may add it to your addressbook under a different name, which now will be displayed as the sender.

Of course, a mail without sender destination (“Anonymous” is displayed as sender) will have two x's.

Clicking one of the e-mails displayed in your inbox will open the mail.

The same applies to all other folders.

(Due to the distributed nature of I2P-Bote, sending as well as checking for and retrieving e-mails takes a few minutes. With mail routes activated respectively more. But you need not keep the browser open for that, simply leave I2P-Bote running as a background process – this is also benefits your anonymity)

2.2.3 Local Address Book

If you have the I2P-Bote e-mail key from somebody you want to write to more frequently, it is handy to store that key locally into your address book (link on the left), specify a name of your own choosing for this contact and paste his mail destination in the corresponding line, then save.

You should normally save destinations to your addressbook, so that next time you get a mail from the same sender it will be shown to be from the same, locally known sender (“Loc” is checked) and a mail sent by someone else who is just using the same user name will be marked as NOT known locally (an x in web-UI's 'Loc' column or [UNK] before the sender address in POP3), so you know it's a new/different one.

2.2.4 Settings (and what they mean)

Under settings you can choose the I2P-Bote interface's *language* (currently English or German) and decide whether even with a non-English language setting everything that will be automatically added to an e-mail when replying will nonetheless stay in English, so that the recipient does not know your I2P-Bote is set to a different language.
Otherwise the recipient could guess about your nationality which would decrease your anonymity.

Here you can also adjust the interval for *automatic checking* of e-mails and decide whether or not to send any *time stamp* with your mails, indicating date and time when the mail was sent. The time stamps are always in UTC.

(When using mail routes, the timestamps are automatically disabled.) [not yet implemented]

automatic checking for e-mails:

For more comfort there is the “Check for mail every XX minutes“ option.

Here you can specify how often your I2P-Bote app should try to fetch unread mails for your identities. This can be set on a per-identity basis [not yet implemented]

If you specify a random offset, then it will not check _exactly_ every XX minutes, but rather every (XX+-offset*XX)minutes, i.e. after a randomly chosen time between (1-offset)XX minutes and (1+offset)XX minutes. [not yet implemented]

You can also totally disable the automatic checking for a given identity.

(If you are not sure about these settings, the defaults should be ok for you.)

Mail routes are chains of I2P-Bote nodes acting as relays/routers for other peers and obeying to per-hop delays, thus providing the high-latency transport for increased anonymity.

You can specify the number of nodes (here called hops) that should be chained to form a mail route. Then each of the e-mail packets sent by the identity that has mail routes enabled will go through a mail route of n hops before being stored. You can set a delay for each hop individually, as no hop should know the time a packet will wait at the next hop, making the timing unpredictable. [individual per-hop and per-identity setting of delays not yet implemented]

As delay you can specify a time frame (e.g. 60-600 minutes) – then a random wait time between the two values will be chosen for the packet at that hop – or a fix time, then the packet will be forwarded at that fix time, e. g. noon UTC, no matter when it arrived. [fix time not yet implemented]

(When using mail routes, the timestamps are automatically disabled. [not yet implemented])

Under “*mínimo en el bote*” (minimum number of relay packets that will be sent) you can specify a threshold. As your node can only act reliably as a mix, if there are enough foreign packets to mix and to blend own packets with, it will accumulate messages who's delay time is over until reaching this lower limit. Only when it is surpassed, your node starts sending them out in random order. [Not yet implemented]

exclude identity from global checking [Not yet implemented]

If you enable this option for one of your identities, then this one will not be affected by the global manual checking for mails nor by any global automatic mail checking.

2.2.5 E-mails to and from the Internet [NOT YET FULLY IMPLEMENTED!]

In order to be able to send bote mails to the internet and to receive e-mails from the internet with your I2P-Bote application, you must first register with an appropriate mail gateway. Currently there is only one: postman.

1) In order to register with postman, go to: http://hq.postman.i2p/?page_id=16 and register an account. If you already have an account or if you have just created one as described, proceed with #2.

2) For an existing account you can add your I2P-Bote mail destination, so that e-mails coming from the internet are forwarded to your I2P-Bote app. To do so go to: http://hq.postman.i2p/?page_id=74 and provide the requested information.

Now all e-mails sent to that address (name@i2pmail.org from the outer internet or name@mail.i2p for mails from other postman subscribers) will be forwarded via the I2P-Bote network to your I2P-Bote app.

(N.B. When using the name@mail.i2p or name@i2pmail.org addresses instead of the long addresses, e-mails are no longer end-to-end encrypted. Therefore, it is recommended to exchange the I2P-Bote mail destination keys for communicating within the network. Postman has offered high quality services in I2P for quite a while already, but be aware that it's a centralized point that might go offline one day, or worse be taken over by an evildoer that will manipulate mails. As for network-internal e-mail communication, I2P-Bote makes sure that if you use the address keys, nobody can tamper with the mails you send or receive.)

If you want not only to receive e-mails from the internet, but also enable sending e-mails from I2P-Bote to the internet, you must provide your I2P-Bote client with the gateway's mail destination key, so that your I2P-Bote knows where to send those mails to.

You can do this under “settings”.

In order to fight abuse, there will be a limitation of the number of e-mails you can send out to the internet; just like for normal postman mail service users: If an I2P-Bote user exceeds the quota with outgoing e-mails, the additional e-mails will be sent back as bounce.

This gateway will allow I2P-Bote users to communicate with the standard e-mail users on the internet as well as with users of postman's classical i2pmail service (@mail.i2p).

3. Considerations about Anonymity

Don't send identifying information about you (name, address, geographic location, time zone, age, websites you have just visited or blogged about, user names, ip numbers, I2P router id, I2P-Bote id, social security number, credit card number, …, copies of your passport, driver's license, home rental contract, photos – nude or with clothes –, documents that contain your username in author's settings, and many many more)!

If possible,

- leave I2P-Bote running 24/7,
- use mailroutes with randomized per-hop delays and/or per-hop fixed send times, [not yet *fully* implemented]
- use a long check interval,
- use a long local delay for own packets,
- use a big check interval randomization. [not yet implemented]

You can suppress the sending of date and time in the e-mails' header.

When you reply to an e-mail, certain markers, such as “Re: [subject of the mail you're replying to]” or “[username] wrote:”. Those are different for the languages you can chose from in your language settings. However, if you don't want the recipient to know what language you have set, you can suppress translation of these markers, so that they will be in English, no matter what you language setting is. In order to do so, mark “Use English for text added to outgoing email ('Re:', 'wrote:', etc.) “

Be careful with the contents you send! Don't include personal information or information that only you can possess. Don't write I'm going to bed now, it's late when including time stamps.

The language in which your write your e-mails, your style and formulations can also be of interest for an attacker.

I2P-Bote also offers the possibility to use different e-mail identities. Suppose one of you contacts learns about your identity, as you forgot to erase identifying information in a secret document you have sent to him. Now if this e-mail's recipient was to collaborate with others you are in contact with, he could tell them the real world identity belonging to the Bote address he knows from you. Thusly, if you communicate with those others using the

same Bote address, they will know who you are.
Not so, if you used a different address for sending mails to them.

4. Concept

I2P-Bote is an end-to-end encrypted, network-internal, fully decentralized (i.e. serverless) e-mail system. It supports different identities and does not expose e-mail headers. Currently, it is still alpha software and can only by accessed via web console. It soon will have POP3 support, and it is planned to guarantee additional anonymity by providing a high-latency transport option. All bote-mails are automatically end-to-end encrypted, so that there's no need to set up extra e-mail encryption (though you can do that), and bote-mails will be authenticated automatically. As it is decentralized, there is no e-mail server that could link different e-mail identities as communicating with each other (*profiling*): Even the nodes relaying the mails will not know the sender and apart from sender and receiver, only the end of the high-latency mail tunnel and the storing nodes will know to whom (anonymous identity) the mail is destined. The original sender can have gone offline, long before the mail becomes available on the other side. This adds on the degree of anonymity that can be reached with I2P-Bote. For those who do not want high delays: All these settings are be user-adjustable, so each user decides on how much anonymity he wants.

I2P-Bote nodes store encrypted e-mails into a Kademlia DHT. Therefore, an e-mail can be sent through a number of other nodes (relays) for increased security, or directly to

a set of storage nodes for faster delivery. The same applies to retrieving email.

(When using mail routes, timestamps are automatically disabled.)
[Retrieving via relays not yet implemented]

All nodes are created equal: There are no "supernodes" or designated relay/storage nodes. Everybody acts as a potential relay and storage node. The maximum amount of disk space used for relayed/stored email packets can be configured by the user.

Before an email is sent to a relay, it is broken up into packets and encrypted with the recipient's public key. These packets are stored redundantly in a distributed hash table (DHT).

They are kept for at least 100 days, during which the recipient can download them.

Relay packets also expire after 100 days or more.

If a node runs out of email storage space, and there are no old packets that can be deleted, the node refuses storage requests.

Furthermore, I2P-Bote sanitizes the mail headers and does not allow any unneeded information to be transmitted, thus allowing the use of e-mail clients without prior checks of what this client sends in the mail headers. [POP3 not yet implemented]

All the encryption, path choosing and profiling is done locally so that there is no trusted party involved.

Using I2P-Bote appropriately, that means keeping in mind the considerations given above and showing some common sense, nobody will be able to find out who or where you are. And if you are already being observed and your internet connection sniffed, the observer will not be able to find out what you send or receive or to whom you are sending to or receiving from or where your contacts are located.

Let's go a bit more into detail:

<u>What I2P-Bote *does hide*:</u>

I2P-Bote hides both, the identity and location of sender and receiver, as well as those of intermediary nodes (relays and storing nodes), the content of your mails, their size, the number of mails you send.

Only the recipient can know the sender's bote mail destination, and if he choses not to send his destination, not even the recipient will know it.

Even if you send time stamps, your time zone will not be disclosed.

Furthermore, I2P-Bote hides ...

- the fact that you run I2P-Bote
- the fact that you send a mail
- the fact that you receive a mail

and hence

- the time you send a mail
- the time you receive a mail

and

- the upper limit of number of mails an unknown user receives, - nota bene: an abstract user, no concrete one, just concluding its existence from the existence of the mail identity - , as he could always have more than one e-mail identity; and the lower limit as an identity also sends out test and dummy messages

What I2P-Bote *hides partially*:

The I2P-Bote address of the recipient will only be known to sender and recipient(s).

In case of multiple recipients, each one will see all other recipients that the mail was addressed to via “To:” or “CC:”.

All entries that were under “BCC:” will only be visible to the sender and this very recipient.

The time an sent time will, if at all, only be visible to sender and recipient.

.

What I2P-Bote *can hide* optionally:

- If mail routes are use, the time a bote mail is sent
- If mail routes are used, the time a bote mail is fetched. [not yet implemented]
- If the sender suppresses timestamps only the sender himself will know when he sent a
  mail.

What I2P-Bote *cannot hide*:

I2P-Bote cannot hide the frequency a given identity checks for new mails nor the number of mails a given identity receives.

Not even for bootstrapping I2P-Bote depends on a central node, as it uses Seedless. [not yet implemented]

5 Terminology/Glossary of Terms:

I2P-Bote (router/node) id:

This is the id an I2P-Bote router is known as. It is used for contacting this router, for storing, relaying and fetching mails, but also used in the hop-to-hop encryption and for simply contacting it via I2P, as it is at the same the I2P-Bote router's I2P tunnel destination. It is displayed to represent an I2P-Bote node in the stats.

So the router id corresponds to the I2P destination (the address of an I2P-Bote node on the I2P network - there is no need to know it unless you are having problems connecting to other I2P-Bote nodes.)

I2P-Bote e-mail destination:

The I2P-Bote e-mail destination (key) is an identifier by which somebody can be reached via I2P-Bote, so as the name states: an e-mail destination. Thus it is for I2P-Bote what an e-mail address is for standard e-mail system: The e-mail destination is the actual address for sending e-mails, for storing them into and for fetching them from the DHT.
At the same time it used for the end-to-end encryption of e-mails, header information and attachments.

An I2P-Bote e-mail destination is a Base64 string containing a public encryption key and a signature verification key. Example:

uQtdwFHqbWHGyxZN8wChjWbCcgWrKuoBRNoziEpE8XDt8koHdJiskYXeUy
q7JmpG

```
  In8WKXY5LNue~62IXeZ-ppUYDdqi5V~
9BZrcbpvgb5tjuu3ZRtHq9Vn6T9hOO1fa
  FYZbK-
FqHRiKm~lewFjSmfbBf1e6Fb~FLwQqUBTMtKYrRdO1d3xVIm2XXK83k1Da
  -
nufGASLaHJfsEkwMMDngg8uqRQmoj0THJb6vRfXzRw4qR5a0nj6dodeBfl2N
gL9
  HfOLInwrD67haJqjFJ8r~vVyOxRDJYFE8
~f9b7k3N0YeyUK4RJSoiPXtTBLQ2RFQ
  gOaKg4CuKHE0KCigBRU-Fhhc4weUzyU-
g~rbTc2SWPlfvZ6n0voSvhvkZI9V52X3

SptDXk3fAEcwnC7lZzza6RNHurSMDMyOTmppAVz6BD8PB4o4RuWq7MQc
nF9znElp
  HX3Q10QdV3omVZJDNPxo-
Wf~CpEd88C9ga4pS~QGIHSWtMPLFazeGeSHCnPzIRYD
```

I2P-Bote router/node id and I2P-Bote e-mail destinations look similar, but are completely independent of each other.

E-mail address:

E-mail addresses in I2P-Bote are shortcuts for e-mail destinations.

The e-mail address <--> e-mail destination mappings are stored in two places: the local address book and the distributed address directory [the latter not yet implemented].

I2P-Bote e-mail identity:

The I2P-Bote e-mail identity is a set of an I2P-Bote e-mail destination key, the corresponding private keys and a name given to it by the user. This name will be sent with the destination key if you do not suppress sending information about the sender.

However it will only be displayed for the recipient in case he does not have a name for this destination in his local address book.

So technically speaking, an e-mail identity consists of four things:

* an e-mail destination (i.e. two public keys)

* two private keys for the e-mail destination

* a public name which can be shown to other people in e-mails

* a description which is not shown to anybody but you.

(It helps you remember which e-mail identity you use for which purpose.)

An e-mail identity is not required for sending emails (although then only "Anonymous" can be selected for the "sender" field).

Mail routes:

Mail routes are an additional high-latency transport for I2P-Bote. For this, a chain of I2P-Bote nodes is built, acting as relays/routers for packets and obeying to individual per-hop delays;[still no individual setting for delays implemented]

BEWARE!

If you choose this option - especially with many hops and / or long delay times, don't be surprised if your mail does not reach its destination too soon. It will, of course, take longer – up to several days!

6. Technical Details

-- see spec --

ENJOY THE BOTE FEELING!!

7. FAQ:

What is I2P-Bote?

I2P-Bote is an end-to-end encrypted, network-internal, fully decentralized (serverless) e-mail system. It supports different identities and does not expose e-mail headers. Currently, it is still alpha software and can only by accessed via web console. It soon will have POP3 support, and it is planned to guarantee additional anonymity by providing a high-latency transport option. All bote-mails are automatically end-to-end encrypted, so that there's no need to set up e-mail encryption (though the option does exist), and bote-mails will be authenticated automatically (authentication not yet implemented). As it is decentralized, there is no e-mail server that could link different e-mail identities as communicating with each other (profiling): Even the nodes relaying the mails will not know the sender and apart from sender and receiver, only the end of the high-latency mail tunnel and the storing nodes will know to whom (anonymous identity) the mail is destined. The original sender can have gone offline, long before the mail becomes available on the other side. This adds on the degree of anonymity that can be reached with I2P-Bote. For those who do not want high delays: All these settings are be user-adjustable, so each user decides on how much anonymity he wants.

Why I2P-Bote?

Because it's cool.

And because I2P was lacking a decentralized e-mail service, and seeing the creation of such as an opportunity to improve on neglected anonymity aspects, it was decided to add an optional high-latency transport.

You can use a normal e-mail account and end-to-end encrypt your mails, but they are still not anonymous.

You can use anonymous server-bound e-mails, yet they are not automatically end-to-end encrypted.
Or you can use I2P-Bote in which your mails are anonymous and AUTOMATICALLY end-to-end-encrypted.
In contrast to standard e-mail systems there is no need to setup an additional key management application. Everything you need is already there.

But despite it being simple and easy to use, it still offers military grade encryption and options for extremely strong anonymity.

How does it work?

-- see the section “Concept” of the Manual –

In short: I2P-Bote nodes form a p2p-network, relaying mail packets for one another and storing them into a DHT.

Why should I use it?

Because you wouldn't go out to the street naked either.

But what do you have to hide? ...

Well maybe you would. But the point is, sometimes you want private e-mail communication to be secret and untraceable. Or you want to communicate fully anonymously with others.

Therefore I2P-Bote is the ideal tool, giving you a lot of flexibility.

It aims to providing professional military grad security and n00b-proof usability:

You can have really paranoid settings, where it takes a mail an eternity to arrive; or have faster communication and still enjoy very high anonymity.

You decide – easily with a mouse click.

How is it better?

WE think it's better for US (and maybe for you; decide yourself!), than …

- mixminion as it is easy to use and as n00b-proof as we could get it.
- anonymous e-mail services not based on destination key routing: as those do not deliver built-in end-to-end encryption.
- centralized services, as the server could go down (due to attacks, legal problems, lack of funding or interest, …) and the server admin has too many means to do profiling.

How is my identity kept safe when I exchange mail with someone?

Never is your ip number or even your I2P-destination included in any e-mail you send.

The high-latency transport counters timing attacks.

End-to-end encryption, per-hop encryption, relaying packets for other nodes, one single packet size* (padding), a constant rate of sending (test and dummy messages)*, and a rather balanced incoming/outgoing ratio* counter traffic analysis attacks, and in combination with per-hop delays, I2P-Bote offers good means against intersection attacks.

The open source nature of I2P-Bote guarantees that you yourself can see the implementation and check it for bugs.

*[not yet implemented]

How do I use it?

Read the manual. If you have questions, ask on the forum:

http://forum.i2p/viewforum.php?f=35

Can I use I2P-Bote with Thunderbird, Evolution, Kmail or ... ?

Yes, you can use the e-mail client of your choice, as long as it supports POP3 and SMTP.

[POP3 not yet implemented]

Does it handle file attachments, and what limits are there?

[not yet implemented]

Can I use GPG with I2P-Bote?

Of course. Either make GPG encrypt your e-mail's text before pasting it into the I2P-Bote mail composition field, or use a mail app with GPG support. [POP3 support not implemented]

How about HTML or styled text?

...

Can it send and receive mail to/from normal internet email servers?

It will very soon.

Can I send mail to postman's traditional I2P mail accounts?

Yes. You can both send and receive mails – very soon.

What is a mail route?

-- see: What does high-latency transport mean?

(When using mail routes, the timestamps are automatically disabled.)

What does high-latency transport mean?

It means that you can enable an option where e-mail packets are not sent directly to storing nodes, but are relayed (forwarded) by other peers (who cannot read the e-mails, as they are encrypted with several layers and ripped into small parts), who do not send them on immediately but wait a user-specified time – in case of sending specified by the sender, in case of receiving specified by recipient.

Therefore it takes the mail some time to arrive. Thus an attacker cannot simply run stats on node uptimes (who was connected when) and times a message was received to be stored (which in a low-latency environment would be about the time it was sent), in order to uncover the real life identities behind I2P-Bote e-mail identities.

What latencies are there, and how can they be controlled (if at all)?

It's distributed and on top of i2p, so it takes some time. Speed is not our strength, but we compare well with other anon mail systems. Without mail routes enabled it takes 3 to 10 minutes from hitting the "Send" button to being displayed in the receiver's inbox.

If speed is what you want, fully disable mail routes or set them to the minimum number of hops and minimum per-hop delay you can live with.

If I2P-Bote generates its own anonymity, why does it need i2p?

I2P-Bote is built on top of i2p mainly for five reasons:

1) I2P was lacking a decentralized e-mail service and HungryHobo is an I2P user.

2) I2P offers very good anonymity, is mature and incorporates years of experience.
So being on top of it, kind of represents an anonymity fall-back even if there were
some crucial bugs in I2P-Bote.

3) Flexibility: We want to offer an easy way to anonymous low-latency e-mail communication as well, with still a high level of protection.

4) I2P traffic blends with I2P-Bote traffic.

5) Even I2P-Bote relays are thus location-hidden.

How anonymous/secure is I2P-Bote without mail routes?

Pretty anonymous and very secure.

It then basically enjoys the anonymity provided by I2P – which is rather strong anonymity already.

However, I2P is a low-latency network, with all the shortcomings a low-latency network comes with by its very nature. There are attacks against which I2P cannot protect you or not protect you very reliably. I2P-Bote does its best to augment I2P anonymity with its high-latency transport option, which make – if enabled – I2P-Bote mails paranoidly anonymous.

What is a bote dest?

There is the I2P-Bote mail identity and an I2P-Bote router id.

The mail identities consist of public and private keys. The public key is the key others use in order to encrypt mails they send to you and in order to verify your signature. It is save to give away that one to anybody you want to get e-mails from. At the same time this public key is a pseudonymous identity. One real user can have more than one of those identities.

It's your address, and therefore it is referred to as a “destination” or short “dest”

It is important to distinguish between the mail dest and the router id!

If you have problems with your and it should be necessary, you can tell your I2P-Bote router id in irc2p, I2P's IRC channels, though until now this has never been necessary. It is not directly linked to your ip.

But nonetheless do NOT relate your I2P-Bote router id with your I2P-Bote mail dests!

Why are the e-mail addresses so long?

In I2P-Bote every mail is encrypted. In order not to require you to exchange an e-mail address _and_ a long key, we simply made that key the address. This comes with two additional benefits: You won't have to worry if an e-mail address is already taken or not (at least not if you do not send or receive e-mails to or from the internet) and you don't need a key management app apart, for taking care of your keys.

It is safe to give away this key, as it is only the public key which everybody may know about without compromising your e-mails' secrecy.

Using the ECC encryption as option will yield shorter e-mail destination keys.

What's the point of multiple mail identities?

I2P-Bote is not an instant messenger, so you can have several identities without having to keep many tunnels open. Only for fetching requests you'd use up more resources but at the same time provide more cover for others.

Or imagine you communicate with your friends unobservedly (see: data retention laws) via I2P-Bote, and want to quickly send out a mail that you'll be meeting each other in a different location tonight. Then, you need no super-anonymity and can renounce mail routes and delays. Your friends, on the other hand, would want to have a shorter check interval, so they will receive the mail in time. Yet still you want super high anonymity for some of your other communications, that's why you have a different identity with mail routes, delays and long check intervals.

What does it mean when UNK/Loc is x'ed for a mail in my inbox?

When the sender's destination is not known locally the mail is marked by an x in the “Loc” column or by putting “[UNK]” before the sender's address in POP3.

This means that you have no proof this user is really who he claims to be, in his user name. Of course, if the signature is valid, you know he possesses the destination key with which the mail was signed, and that the mail content is from that person. But you cannot rely on the short name here. In case you had gotten a mail from a user with this name before, you cannot be sure it is the same user this time, even if signature is ok.

In this case you must compare the destination keys or add them to your addressbook.

So user not locally known, are not intrinsically bad or evil, but you shouldn't trust it's the user you might think it is. But, if verified against locally stored keys, you know it's the same user when you receive another mail from him and “Loc” has a green check.

What can I do to be more anonymous?

- Don't send identifying information about you! (name, address, photos, geographic location, time zone, age, sex, websites, login names, I2P router id, I2P-Bote id, Files that contain author information about you, …)
- don't send personal information or information that only you can possess,
- leave I2P-Bote running 24/7,
- use mailroutes with randomized per-hop delays and/or per-hop fixed send times, [not yet fully implemented]
- use a long check interval,
- use a long local delay for own packets,
- use a big check interval randomization. [not yet implemented]

- suppress the sending of date and time in the e-mails' header,
- suppress translation of markers like “Re:” into another language,
- watch your language and writing style,
- use different e-mail identities,
- Consider discarding e-mail identities after longer periods of usage,
- **...**

How do I not send my timestamps?

Go to settings and disable sending of timestamps. This will have the effect that your mail will not contain a date or time of sending.

(When using mailroutes, the timestamps are automatically disabled.)

Is I2P-Bote open source?

Of course!

“This software is licensed under the GPL version 3 (see licenses/GPLv3.txt),

except for bcprov-ecc-jdk16-145.jar which is licensed under the

Bouncy Castle License (see licenses/BouncyCastle.txt).”

What do “BktPfx”, “Distance” and “Locked?” mean?

- BktPfx=BucketPrefix

- Distance: the distance of an I2P-Bote node to your own node in keyspace

- Locked: If a node is not reachable for whatever reason, it is marked as locked, plus the time it has been found unreachable.

Who made I2P-Bote?

Conception, technical design, implementation and web user interface were/are done by HungryHobo, an anonymous developer.

For feedback or if you want to offer help, you can contact him using I2P-Bote. His destination key is:

```
hobo37SEJsEMfQHwcpVlvEgnrERGFz34GC1yjVyuRvl1QHnTi0UAoOtrL
P~qkFY0oL59BBqj5sCep0RA8I5G8n
```

Credits:

Idea: HungryHobo

Technical concept: HungryHobo, mixxy

Implementation: HungryHobo

Plugin support: zzz, HungryHobo

User interface: HungryHobo, dr|z3d

Seedless integration: sponge

German translation: HungryHobo

Alpha testing: HungryHobo, mixxy, Returning Novice, sponge, and many others

I2P-Bote Manual

1. Introduction

I2P-Bote is an easy-to-use, highly anonymous secure e-mail application for I2P. It is a serverless, fully decentralized system that establishes/forms a peer-to-peer network built on top of state-of-the-art low latency anonymizing network I2P; adding to it an optional mixminion-like high-latency transport and thus avoiding the shortcomings of low-latency networks.

Therefore, I2P-Bote makes full use of the anonymity provided by I2P, plus it generates its own anonymity by adding another anonymizing layer (overlay network).

This concept of layered anonymity is what makes I2P-Bote so flexible:

You can configure it to be extremely anonymous and slow or less anonymous but faster/more efficient. In any event, I2P-Bote always provides a very good anonymity for both, sender and receiver, as well as end-to-end encryption*.

I2P-Bote offers the option to make your communications even more anonymous, by enabling the high-latency mail routes – at cost of performance, however. Users that want their anonymous e-mails to arrive as quickly as possible, will want to disable the mail routes and use 'direct' sending through I2P. It is guaranteed that you will never be less anonymous than the anonymity provided by standard I2P connections.

In order to achieve high usability, we have enabled it to be used with standard mail clients such as Thunderbird, Evolution or Kmail, without having to worry about what extra information these applications send in their headers. [YET TO BE IMPLEMENTED] Furthermore there is a web interface that lets you send and read e-mails or manage your settings and identities.

I2P-Bote is easy to use: If you're not yet using I2P, just install I2P from http://www.i2p2.de and then install the I2P-Bote plugin as described in this manual. Otherwise simply read on!**

Current version is 0.2.5.

*Unless you send e-mails to or receive them from the regular internet, ALL emails – the mail body, attachments and the header except recipient's address (subject, date, time, sender address, ...) are automatically and transparently end-to-end encrypted. The recipient's address is only visible for the mail route's last node that stores the packets into the kad network, and the respective storing nodes, but they cannot read the mail's content nor who sent it nor who will fetch it.

**Of course you can also compile from source.

2. Howto

2.1. Installation

In order to install I2P-Bote, go to the bottom of the I2P Client Configuration page at

http://localhost:7657/configclients.jsp

and enter:

http://tjgidoycrw6s3guetge3kvrvynppqjmvqsosmtbmgqasa6vmsf6a.b32.i2p/i2pbote.xpi2p

(http://i2pbote.i2p/i2pbote.xpi2p might work, too, if you have i2pbote.i2p in your address book or a subscription)

in the “Plugin Installation Download Url” line, then hit “Install Plugin”. Wait until your sidebar says plugin installed and started.

In order to update your I2P-Bote instance, click 'Update' under I2P-Bote on the I2P Client Configuration page at http://localhost:7657/configclients.jsp

2.2. Using I2P-Bote

On your router console http://127.0.0.1:7657/ click on *SecureMail* on the upper left (in the sidebar). Now you are on I2P-Bote's web interface.

After starting I2P-Bote (by default it is set to start automatically when your I2P router starts up) it takes a bit more than three minutes for everything to be up and running.

So have a look at 'Network Status' on the left. It should state 'Connected'.

If you want to use I2P-Bote for yourself, you first need to create an identity.

2.2.1 Creating an Identity

Click on 'Identities' on the left, then hit the “New Identity” button.

Enter at least a 'Public Name' and hit 'Create'. That's all that's needed to create an identity.

The public name is the name you see for this identity (useful in case you have different identities for different sets of users you communicate with or different purposes) and it will be sent as “sender's name” to the mail's recipient. There is no need for Public Name to be unique.

(As you can choose any name here – anyone could call himself HungryHobo there – it is not suited to be used by the recipient for telling if two mails come from the same sender. This is why the name saved in the local addressbook (there can only by one name per destination key) is displayed, if there is any, and you will see a green mark in the “Know” column, stating it is the locally known name. If there is no entry for a destination in local addressbook, the name specified by the sender will be displayed with a prefixed [UNK] in the mail clients). [POP3 NOT YET IMPLEMENTED]

You can also fill out the other fields, if you like:

Description – this field is kept locally. It's just for your convenience: If you want to add some additional information for yourself about that identity, you can enter it here.

Email Address – this field is not used yet.

Choose from one of the given encryption algorithms. If in doubt, stick to the defaults.

You click on the name of one of your identities and copy the long key displayed under 'Email Destination'. This is your I2P-Bote e-mail address. If you want anybody to be able to send you a bote mail, he need to be given this long key.

Now you can send and receive I2P-Bote mails.

But you should also have a look at your I2P-Bote settings and see if they fit your needs.

(You can also create various identities and assign different settings to each of them.)

2.2.2 Sending and Receiving E-Mails

You need to have the I2P-Bote e-mail destination key of the user you to whom you want to send a bote mail.

In order to send a message, click on 'New', choose your own sender identity or 'Anonymous' under “From” and enter the recipient's e-mail destination key or alternatively an address in the “To:” line.

Alternatively, you can hit the “Addr. Book” button right under this very line, in order to chose from e-mail dests stored locally in your address book: Mark the user(s) to which you want your mail to be sent and hit the “Add Recipients” button.)

You can add several recipients and change the 'To:' to 'CC:' or 'BCC:'.

The “+” button adds additional recipient lines.

Now write your bote mail and hit 'Send' for sending it, or 'Save' in order to store it as a draft into your 'drafts' folder or any user-defined folder. [not yet implemented]

Hitting “Send” will place your e-mail into the Outbox folder and you can go on using I2P-Bote, e.g. writing another e-mail, or simply do other things. I2P-Bote is now sending your e-mail. Once it is sent, it's automatically removed from Outbox and stored into your Sent folder. This means, your mail is entirely on the way to its destination (unless you have set a delay time, which is disabled by default).

In I2P-Bote e-mails are automatically signed (unless send without any sender identity).
You can also send e-mails without specifying *any* sender identity/destination/address, just select “Anonymous” in the scroll-down menu “From:”.

In the default settings I2P-Bote will automatically check for new mails, and all you need to do in order to see if you got e-mails is look into your Inbox (link 'Inbox' on the left).
You can force a manual check by clicking the 'Check Mail' button. This is a global checking, that tries to fetch new mails for all of

your identities, except for those you have excluded from global checking. [not yet implemented]

The number of unread e-mails is shown in parenthesis next to the folder's name in the sidebar.

Click on “Inbox” to have a list of received e-mails displayed. You will see two columns with x's or green checks. Those show you if a mail contains a valid signature and is thus authentic (Sig) and if the sender's e-mail destination key is locally known, i.e. in your addressbook (Know). Hence, two green checks next to a mail entry mean that you already know that e-mail identity and that the mail is signed by that identity.

If you have a certain name in your address book and you get a mail from an identity with that name, yet Know is *not* displaying a green check, then it is a *different* destination that sent and signed this mail; he simply has chosen the same name you have chosen for one of your contacts.

Is there a green check mark for “Sig”, then the mail is correctly signed by the sender and you may add it to your addressbook under a different name, which now will be displayed as the sender.

Of course, a mail without sender destination (“Anonymous” is displayed as sender) will have two x's.

Clicking one of the e-mails displayed in your inbox will open the mail.

The same applies to all other folders.

(Due to the distributed nature of I2P-Bote, sending as well as checking for and retrieving e-mails takes a few minutes. With mail routes activated respectively more. But you need not keep the browser open for that, simply leave I2P-Bote running as a background process – this is also benefits your anonymity)

2.2.3 Local Address Book

If you have the I2P-Bote e-mail key from somebody you want to write to more frequently, it is handy to store that key locally into your address book (link on the left), specify a name of your own choosing for this contact and paste his mail destination in the corresponding line, then save.

You should normally save destinations to your addressbook, so that next time you get a mail from the same sender it will be shown to be from the same, locally known sender (“Loc” is checked) and a mail sent by someone else who is just using the same user name will be marked as NOT known locally (an x in web-UI's 'Know' column or [UNK] before the sender address in POP3), so you know it's a new/different one.

2.2.4 Settings (and what they mean)

Under settings you can choose the I2P-Bote interface's *language* (currently English or German) and decide whether even with a non-English language setting everything that will be automatically added to an e-mail when replying will nonetheless stay in English, so that the recipient does not know your I2P-Bote is set to a different language.
Otherwise the recipient could guess about your nationality which would decrease your anonymity.

Here you can also adjust the interval for *automatic checking* of e-mails and decide whether or not to send any *time stamp* with your mails, indicating date and time when the mail was sent. The time stamps are always in UTC.

(When using mail routes, the timestamps are automatically disabled.) [not yet implemented]

automatic checking for e-mails:

For more comfort there is the “Check for mail every XX minutes“ option.

Here you can specify how often your I2P-Bote app should try to fetch unread mails for your identities. This can be set on a per-identity basis [not yet implemented]

If you specify a random offset, then it will not check _exactly_ every XX minutes, but rather every (XX+-offset*XX)minutes, i.e. after a randomly chosen time between (1-offset)XX minutes and (1+offset)XX minutes. [not yet implemented]

You can also totally disable the automatic checking for a given identity.

(If you are not sure about these settings, the defaults should be ok for you.)

Mail routes are chains of I2P-Bote nodes acting as relays/routers for other peers and obeying to per-hop delays, thus providing the high-latency transport for increased anonymity.

You can specify the number of nodes (here called hops) that should be chained to form a mail route. Then each of the e-mail packets sent by the identity that has mail routes enabled will go through a mail route of n hops before being stored. You can set a delay for each hop individually, as no hop should know the time a packet will wait at the next hop, making the timing unpredictable. [individual per-hop and per-identity setting of delays not yet implemented]

As delay you can specify a time frame (e.g. 60-600 minutes) – then a random wait time between the two values will be chosen for the packet at that hop – or a fix time, then the packet will be forwarded at that fix time, e. g. noon UTC, no matter when it arrived. [fix time not yet implemented]

(When using mail routes, the timestamps are automatically disabled. [not yet implemented])

Under “*mÃnimo en el bote*” (minimum threshold number of relay packets that will be sent) you can specify a threshold. As your node can only act reliably as a mix, if there are enough foreign packets to mix and to blend own packets with, it will accumulate messages who's delay time is over until reaching this lower limit. Only when it is surpassed, your node starts sending them out in random order. [Not yet implemented]

exclude identity from global checking [Not yet implemented]

If you enable this option for one of your identities, then this one will not be affected by the global manual checking for mails nor by any global automatic mail checking.

2.2.5 E-mails to and from the Internet [NOT YET FULLY IMPLEMENTED!]

In order to be able to send bote mails to the internet and to receive e-mails from the internet with your I2P-Bote application, you must first register with an appropriate mail gateway. Currently there is only one: postman.

1) First, go to: http://hq.postman.i2p/?page_id=16 and register an account. If you already have an account or if you have just created one as described, proceed with #2.

2) For an existing account you can add your I2P-Bote mail destination, so that e-mails coming from the internet are forwarded to your I2P-Bote app. To do so go to: http://hq.postman.i2p/?page_id=74 and provide the requested information.

Now all e-mails sent to that address (name@i2pmail.org from the outer internet or name@mail.i2p for mails from other postman subscribers) will be forwarded via the I2P-Bote network to your I2P-Bote app.

(N.B. When using the name@mail.i2p or name@i2pmail.org addresses instead of the long addresses, e-mails are no longer end-to-end encrypted. Therefore, it is recommended to exchange the I2P-Bote mail destination keys for communicating within the network. Postman has offered high quality services in I2P for quite a while already, but be aware that it's a centralized point that might go offline one day, or worse be taken over by an evildoer that will manipulate mails. As for network-internal e-mail communication, I2P-Bote makes sure that if you use the address keys, nobody can tamper with the mails you send or receive.)

If you want not only to receive e-mails from the internet, but also enable sending e-mails from I2P-Bote to the internet, you must provide your I2P-Bote client with the gateway's mail destination key, so that your I2P-Bote knows where to send those mails to. You can do this under “settings”. This gateway will allow I2P-Bote users to communicate with the standard e-mail users on the internet as well as with users of postman's classical i2pmail service (@mail.i2p).

In order to fight abuse, there will be a limitation of the number of e-mails you can send out to the internet; just like for normal postman mail service users: If an I2P-Bote user exceeds the quota with outgoing e-mails, the additional e-mails will be sent back as bounce.

3. Considerations about Anonymity

Don't send identifying information about you (name, address, geographic location, time zone, age, websites you have just visited or blogged about, user names, ip numbers, I2P router id, I2P-Bote id, social security number, credit card number, …, copies of your passport, driver's license, home rental contract, photos – nude or with clothes –, documents that contain your username in author's settings, and many many more)!

If possible,

- leave I2P-Bote running 24/7,
- use mailroutes with randomized per-hop delays and/or per-hop fixed send times, [not yet *fully* implemented]
- use a long check interval,
- use a long local delay for own packets,
- use a big check interval randomization. [not yet implemented]

You can suppress the sending of date and time in the e-mails' header.

When you reply to an e-mail, certain markers, such as “Re: [subject of the mail you're replying to]” or “[username] wrote:”. Those are different for the languages you can chose from in your language settings. However, if you don't want the recipient to know what language you have set, you can suppress translation of these markers, so that they will be in English, no matter what you language setting is. In order to do so, mark “Use English for text added to outgoing email ('Re:', 'wrote:', etc.) “

Be careful with the contents you send! Don't include personal information or information that only you can possess. Don't write I'm going to bed now, it's late when including time stamps.
The language in which your write your e-mails, your style and formulations can also be of interest for an attacker.

I2P-Bote also offers the possibility to use different e-mail identities.
Suppose one of you contacts learns about your identity, as you forgot to erase identifying information in a secret document you have sent to him. Now if this e-mail's recipient was to collaborate with others you are in contact with, he could tell them the real world identity belonging to the Bote address he knows from you. Thusly, if you communicate with those others using the same Bote address, they will know who you are.
Not so, if you used a different address for sending mails to them.

4. Technical Concept

I2P-Bote is an end-to-end encrypted, network-internal, fully decentralized (i.e. serverless) e-mail system. It supports different identities and does not expose e-mail headers. Currently, it is still alpha software and can only by accessed via web console. It soon will have POP3 support, and it is planned to guarantee additional anonymity by providing a high-latency transport option. All bote-mails are automatically end-to-end encrypted, so that there's no need to set up extra e-mail encryption (though you can do that), and bote-mails will be authenticated automatically. As it is decentralized, there is no e-mail server that could link different e-mail identities as communicating with each other (*profiling*): Even the nodes relaying the mails will not know the sender and apart from sender and receiver, only the end of the high-latency mail tunnel and the storing nodes will know to whom (anonymous identity) the mail is destined. The original sender can have gone offline, long before the mail becomes available on the other side. This adds on the degree of anonymity that can be reached with I2P-Bote. For those who do not want high delays: All these settings are be user-adjustable, so each user decides on how much anonymity he wants.

I2P-Bote nodes store encrypted e-mails into a Kademlia DHT. Therefore, an e-mail can be sent through a number of other nodes (relays) for increased security, or directly to a set of storage nodes for faster delivery. The same applies to retrieving email. (When using mail routes, timestamps are automatically disabled.)
[Retrieving via relays not yet implemented]

All nodes are created equal: There are no "supernodes" or designated relay/storage nodes. Everybody acts as a potential relay and storage node. The maximum amount of disk space used for relayed/stored email packets can be configured by the user.

Before an email is sent to a relay, it is broken up into packets and encrypted with the recipient's public key. These packets are stored redundantly in a distributed hash table (DHT).

They are kept for at least 100 days, during which the recipient can download them.

Relay packets also expire after 100 days or more.

If a node runs out of email storage space, and there are no old packets that can be deleted, the node refuses storage requests.

Furthermore, I2P-Bote sanitizes the mail headers and does not allow any unneeded information to be transmitted, thus allowing the use of e-mail clients without prior checks of what this client sends in the mail headers. [POP3 not yet implemented]

All the encryption, path choosing and profiling is done locally so that there is no trusted party involved.

Using I2P-Bote appropriately, that means keeping in mind the considerations given above and showing some common sense, nobody will be able to find out who or where you are. And if you are already being observed and your internet connection sniffed, the observer will not be able to find out what you send or receive or to whom you are sending to or receiving from or where your contacts are located.

Let's go a bit more into detail:

What I2P-Bote *does hide*:

I2P-Bote hides both, the identity and location of sender and receiver, as well as those of intermediary nodes (relays and storing nodes), the content of your mails, their size, the number of mails you send.

Only the recipient can know the sender's bote mail destination, and if he choses not to send his destination, not even the recipient will know it.

Even if you send time stamps, your time zone will not be disclosed.

Furthermore, I2P-Bote hides ...

- the fact that you run I2P-Bote
- the fact that you send a mail
- the fact that you receive a mail

  and hence

- the time you send a mail
- the time you receive a mail

  and

- the upper limit of number of mails an unknown user receives, - nota bene: an abstract
  user, no concrete one, just concluding its existence from the existence of the mail identity
- as he could always have more than one e-mail identity; and the lower limit as an
  identity also sends out test and dummy messages

What I2P-Bote *hides partially*:

The I2P-Bote address of the recipient will only be known to sender and recipient(s).

In case of multiple recipients, each one will see all other recipients that the mail was addressed to via “To:” or “CC:”.

All entries that were under “BCC:” will only be visible to the sender and this very recipient.

The time an sent time will, if at all, only be visible to sender and recipient.

What I2P-Bote *can hide* optionally:

- If mail routes are use, the time a bote mail is sent
- If mail routes are used, the time a bote mail is fetched. [not yet implemented]
- If the sender suppresses timestamps only the sender himself will know when he sent a mail.

What I2P-Bote *cannot hide*:

I2P-Bote cannot hide the frequency a given identity checks for new mails nor the number of mails a given identity receives.

Not even for bootstrapping I2P-Bote depends on a central node, as it uses Seedless.

5 Terminology/Glossary of Terms:

I2P-Bote (router/node) id:

This is the id an I2P-Bote router is known as. It is used for contacting this router, for storing, relaying and fetching mails, but also used in the hop-to-hop encryption and for simply contacting it via I2P, as it is at the same the I2P-Bote router's I2P tunnel destination. It is displayed to represent an I2P-Bote node in the stats.

So the router id corresponds to the I2P destination (the address of an I2P-Bote node on the I2P network - there is no need to know it unless you are having problems connecting to other I2P-Bote nodes.)

I2P-Bote e-mail destination:

The I2P-Bote e-mail destination (key) is an identifier by which somebody can be reached via I2P-Bote, so as the name states: an e-mail destination. Thus it is for I2P-Bote what an e-mail address is for standard e-mail system: The e-mail destination is the actual address for sending e-mails, for storing them into and for fetching them from the DHT.
At the same time it used for the end-to-end encryption of e-mails, header information and attachments.

An I2P-Bote e-mail destination is a Base64 string containing a public encryption key and a signature verification key. Example:

uQtdwFHqbWHGyxZN8wChjWbCcgWrKuoBRNoziEpE8XDt8koHdJiskYXeUyq7JmpG

In8WKXY5LNue~62IXeZ-ppUYDdqi5V~9BZrcbpvgb5tjuu3ZRtHq9Vn6T9hOO1fa

FYZbK-FqHRiKm~lewFjSmfbBf1e6Fb~FLwQqUBTMtKYrRdO1d3xVIm2XXK83k1Da

-nufGASLaHJfsEkwMMDngg8uqRQmoj0THJb6vRfXzRw4qR5a0nj6dodeBfl2NgL9

HfOLlnwrD67haJqjFJ8r~vVyOxRDJYFE8~f9b7k3N0YeyUK4RJSoiPXtTBLQ2RFQ

gOaKg4CuKHE0KCigBRU-Fhhc4weUzyU-g~rbTc2SWPlfvZ6n0voSvhvkZl9V52X3

SptDXk3fAEcwnC7lZzza6RNHurSMDMyOTmppAVz6BD8PB4o4RuWq7MQcnF9znElp

HX3Q10QdV3omVZJDNPxo-Wf~CpEd88C9ga4pS~QGlHSWtMPLFazeGeSHCnPzlRYD

I2P-Bote router/node id and I2P-Bote e-mail destinations look similar, but are completely independent of each other.

E-mail address:

E-mail addresses in I2P-Bote are shortcuts for e-mail destinations.

The e-mail address <--> e-mail destination mappings are stored in two places: the local address book and the distributed address directory [the latter not yet implemented].

I2P-Bote e-mail identity:

The I2P-Bote e-mail identity is a set of an I2P-Bote e-mail destination key, the corresponding private keys and a name given to it by the user. This name will be sent with the destination key if you do not suppress sending information about the sender.

However it will only be displayed for the recipient in case he does not have a name for this destination in his local address book.

So technically speaking, an e-mail identity consists of four things:

* an e-mail destination (i.e. two public keys)

* two private keys for the e-mail destination

* a public name which can be shown to other people in e-mails

* a description which is not shown to anybody but you.

(It helps you remember which e-mail identity you use for which purpose.)

An e-mail identity is not required for sending emails (although then only "Anonymous" can be selected for the "sender" field).

Mail routes:

Mail routes are an additional high-latency transport for I2P-Bote. For this, a chain of I2P-Bote nodes is built, acting as relays/routers for packets and obeying to individual per-hop delays; [still no individual setting for delays implemented]

BEWARE!

If you choose this option - especially with many hops and / or long delay times, don't be surprised if your mail does not reach its destination too soon. It will, of course, take longer – up to several days!

6. Credits

Idea & technical concept: HungryHobo, Mixxy

Implementation: HungryHobo

Plugin support: zzz, HungryHobo

User interface: HungryHobo

Seedless integration: sponge

German translation: HungryHobo

French translation: albat, Redzara, Mixxy

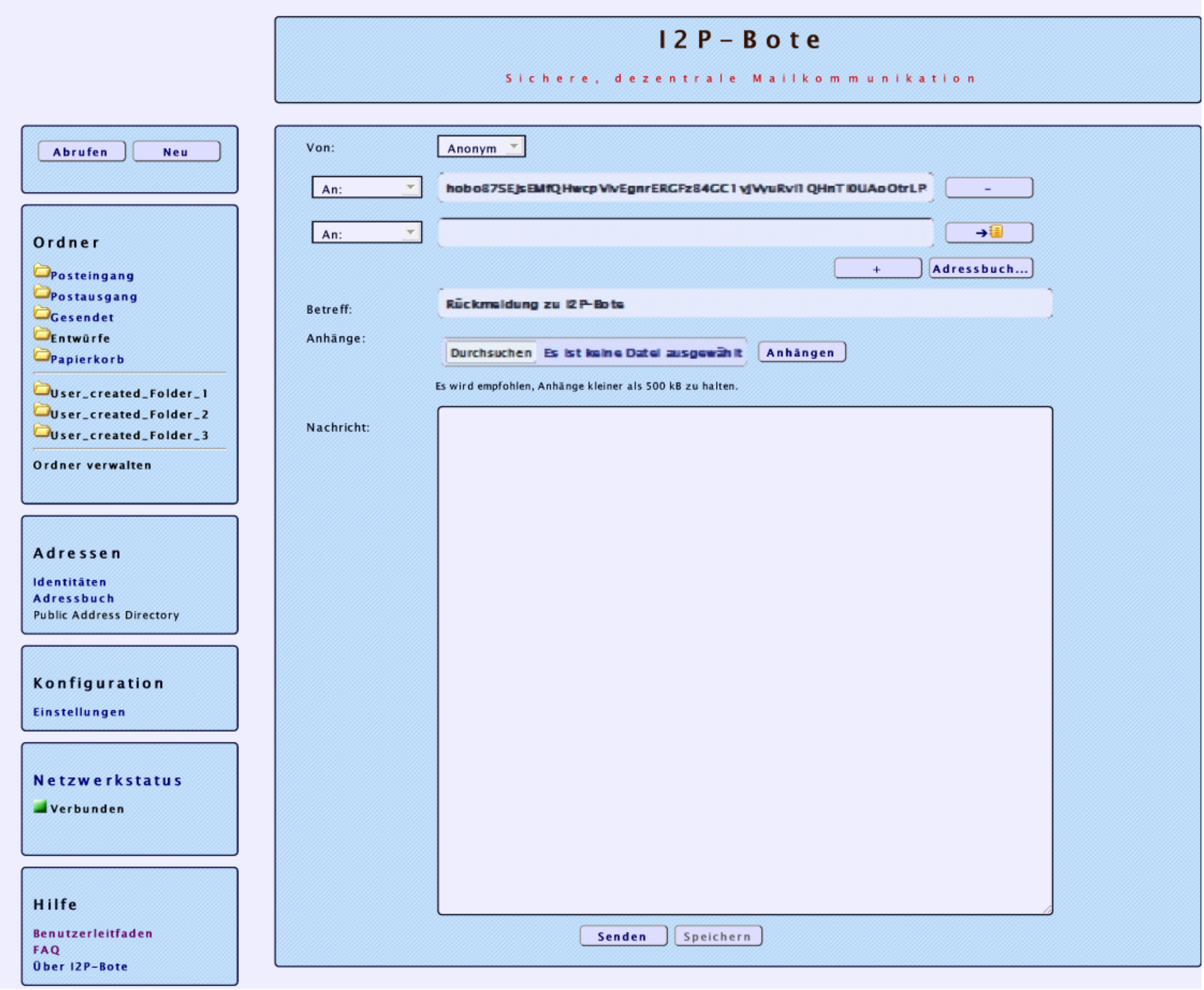
Spanish translation: Mixxy

Alpha testing: HungryHobo, Mixxy, Returning Novice, sponge, and many others

7. Technical Details

-- see techdoc.txt --

ENJOY THE BOTE FEELING!!



Von: Anonym

An: hobo87SEJsEMfQHwcpVlvEgnrERGFz84GC1vjWvuRvI1QHnTIDUAoOtrLP

An:

Betreff: Rückmeldung zu I2P-Bote

Anhänge: Es ist keine Datei ausgewählt

Es wird empfohlen, Anhänge kleiner als 500 kB zu halten.

Hi!

Distributed email service on I2P

I2PBote is a distributed email system running on I2P. It includes technics like kademlia and else.
A documentation is available, to: documentation.txt.

Latest version is 0.2.6, fetchable as a plugin for the plugin system of I2P via i2pbote.i2p
Or fetch it from my eepsite:
i2pbote.xpi2p, currently 0.2.6
i2pbote 0.2.6 src
SHA256sum of 0.2.6 src.zip: 1e6caf9cf25030fcac2268d8b191b954ee6da9feac9edd9d31c0516a236450ef

Version 0.2.5:
i2pbote.xpi2p, currently 0.2.5
i2pbote 0.2.5 src
SHA256sum of 0.2.5 src.zip: 212829601facabaacfb761049862235789952f887a9b235abf76c05472d3f812

Version 0.2.3:
i2pbote.xpi2p
i2pbote 0.2.3 src
SHA256sum of 0.2.3 src.zip: c9dc12c592c91d09f41e8cc226a916c4b5dcaa0187e54b13dfde7b3b30936dbe

Version 0.2.2:
i2pbote 0.2.2 src
SHA256sum of 0.2.2 src.zip: 5d849d98fcebaca4954bf031b203e3a5c0fde93080b785b5bb5293c44f4f29c1
i2pbote.war
SHA256sum of 0.2.2 i2pbote.war: 3fdcd54c8b4ef8da20788528f8df4bcb6977e7308a8c3f6955fab39379919753

Version 0.2:
0.2.zip archive
SHA256sum of 0.2.zip: e03352c640a486c382a6064c9bf211253210c859b6e1b0f3c6043ddbcbd1f808
0.2.i2pbote.war
SHA256sum of 0.2.i2pbote.war: 20395ba1c7a15ced8c10510f45066c39d78edc1db6ac39b6eaeff969449f464f

A quick HowTo copied out of forum:

Current version let you do the following stuff:
* create email identities
* send emails
* receive emails

Be aware that this is very pre-alpha code. It may spit in your breakfast, take your childrens' toys away, etc. etc. You are encouraged to download the source at http://i2pbote.i2p/releases/0.1.2/src.zip and examine it for malicious or insecure code. You can then build the .war file yourself by running ant in the same directory as build.xml.

Or, if you trust me enough and just want to try it out, follow these steps:

1. Download i2pbote.war here: http://i2pbote.i2p/
2. Copy i2pbote.war to (I2P base)/webapps
3. Go to http://localhost:7657/configclients.jsp
4. Under "Web app configuration", check that i2pbote is displayed. If it is not running, click the "Start" button next to "i2pbote". If i2pbote doesn't show up, restart the router.
5. Wait until you get a message saying "WebApp i2pbote started."
6. Clicking on the "i2pbote" link in the message will take you to the I2P-Bote web interface.
7. The k-peers number under Network Status should initially be 0, then go up to 1 or more.

Email addresses look a lot like I2P destinations. They are tied to email destinations, which you can create on the identities page.
If you want to send me a test email, use the following address:

uQtdwFHqbWHGyxZN8wChjWbCcgWrKuoBRNoziEpE8XDt8koHdJiskYXeUyq7JmpGln8WKXY5LNue~62IXeZ-
ppUYDdqi5V~9BZrcbpvgb5tjuu3ZRtHq9Vn6T9hOO1faFYZbK-
FqHRiKm~lewFjSmfbBf1e6Fb~FLwQqUBTMtKYrRdO1d3xVIm2XXK83k1Da-
nufGASLaHJfsEkwMMDngg8uqRQmoj0THJb6vRfXzRw4qR5a0nj6dodeBfl2NgL9HfOLlnwrD67haJqjFJ8r~vVyOxRDJYFE8~f9b7k3N0YeyUK4RJSoiPXtTBLQ2RFQgOaKg4CuKHE0KCigBRU-
Fhhc4weUzyU-
g~rbTc2SWPlfvZ6n0voSvhvkZl9V52X3SptDXk3fAEcwnC7lZzza6RNHurSMDMyOTmppAVz6BD8PB4o4RuWq7MQcnF9znElpHX3Q10QdV3omVZJDNPxo-
Wf~CpEd88C9ga4pS~QGlHSWtMPLFazeGeSHCnPzlRYD

If you want me to reply, create an email identity first and include it in your email. You can also send email to yourself, of course.

One more thing: You'll notice it takes a long time to send and receive emails. I hope to improve this in the next version.

Old versions:
0.1.5:
0.1.5.zip archive
SHA256sum of 0.1.5.zip: febd3f87015d6501b5680235a80c69f12593f87e2be9141b8516ede8c9ca968d

0.1.2 i2pbote.war
MD5sum of i2pbote.war: e894937b9b89f6ff224f5f3fbfaa7eeb
SHA256 of i2pbote.war: e550a8861a27b2a57402810df6aed199b9c578294db858c4ce06e69026896f9a

I2P-Bote

Secure Distributed Email

- HOME
- DOWNLOAD
- SCREENSHOTS
- USER GUIDE
- FAQ
- FORUM
- CONTACT

Instructions for new users:

If you are using Windows, download and run this installer. It will install I2P and I2P-Bote. After installation, run I2P and give it a few minutes to integrate itself into the network. Then click the link that says "SecureMail" in the top left corner of the router console.

If you are using an operating system other than Windows, follow these steps:

1. If you don't have I2P installed yet, get it from http://www.i2p2.i2p/download.
2. Once I2P is running, go to the I2P Client Configuration page and scroll all the way to the bottom.
3. Under "Plugin Installation", copy and paste the following URL into the text field:
   `http://tjgidoycrw6s3guetge3kvrvynppqjmvqsosmtbmgqasa6vmsf6a.b32.i2p/i2pbote.xpi2p`
4. Click the "Install Plugin" button and give it a minute to download the plugin. It will start automatically.
5. When you see a link that says "SecureMail" in the top left corner of the page, the installation is complete.

Updating an existing installation:

- Go to the I2P Client Configuration page and click "Check for updates".

Source code:

src.zip, version 0.2.5
`SHA256: 212829601facabaacfb76104986223578995 2f887a9b235abf76c05472d3f812`
The source contains an Ant build file.

Version history:

history.txt

CSS: David Herreman

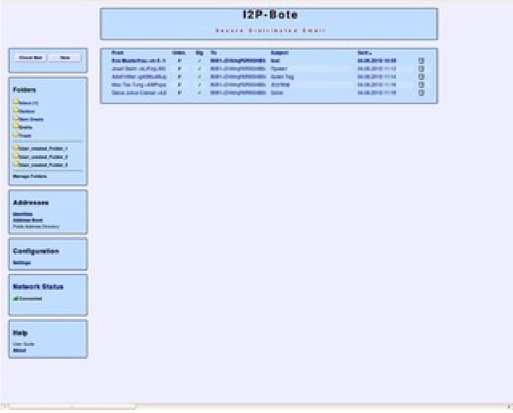
XHTML - CSS

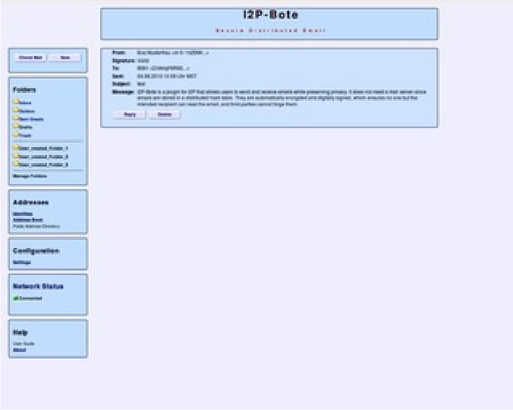
I2P-Bote

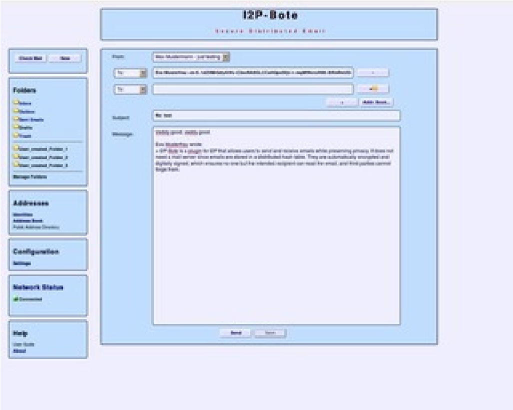
Secure Distributed Email

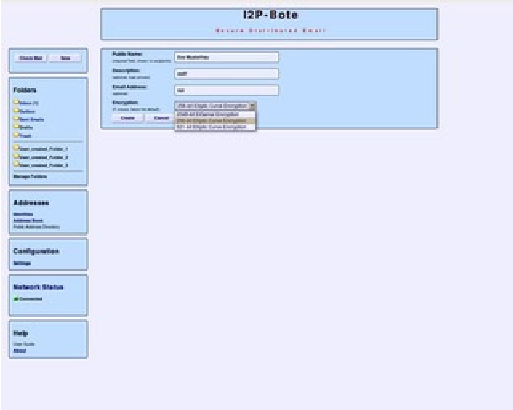
- HOME
- DOWNLOAD
- SCREENSHOTS
- USER GUIDE
- FAQ
- FORUM
- CONTACT

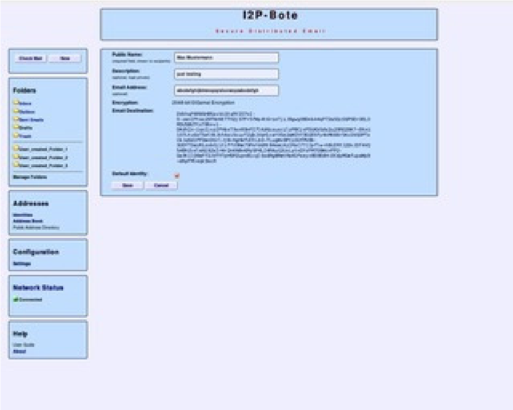
Screenshots

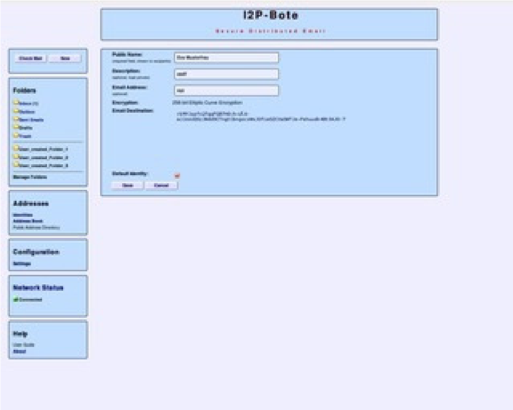


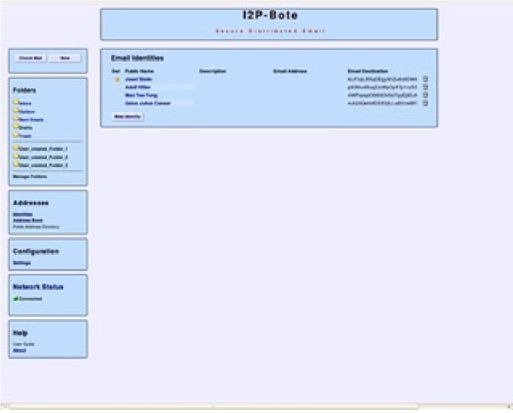






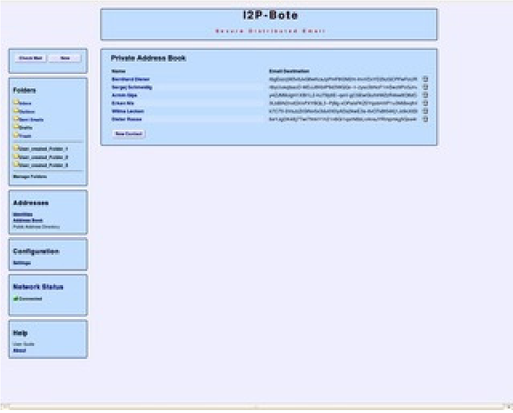






Email Identities

Def	Public Name	Description	Email Address	Email Destination
☆	Josef Stalin			[illegible]
	Adolf Hitler			[illegible]
	Mao Tse-Tung			[illegible]
	Gaius Julius Caesar			[illegible]



Private Address Book

Name	Email Destination
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

CSS: David Herreman

XHTML - CSS

I2P-Bote

Secure Distributed Email

- HOME
- DOWNLOAD
- SCREENSHOTS
- USER GUIDE
- FAQ
- FORUM
- CONTACT

Frequently Asked Questions

What is I2P-Bote?
A peer-to-peer email program designed to protect your privacy.

Why is it named I2P-Bote?
Bote is the German word for messenger.

What happens with an email after I click "Send"?
It is encrypted and stored on other I2P-Bote participants' computers. From there, it is delivered to the recipient when they check their email.

Wait a minute, all email I send is saved on some random person's hard drive? That sounds like a really dumb idea!
All they see is garbage data because it is encrypted with "military-grade" encryption. Only you and the recipient know what is in the email. Additionally, if you send the email with relays enabled, it is not even possible to tell who sent it.
Between this and using an email account with a company that doesn't respect your privacy, over an internet line that is being spied on by shady agencies, which would you say is more trustworthy?

What about PGP and GPG?
PGP and GPG let you encrypt email and send it through your existing email account. They offer strong encryption, but they only encrypt the email text, not the headers, which means the subject line, your computer name, and other information is not secure. Another privacy issue is that PGP/GPG cannot prevent anybody from finding out who is talking to who.
I2P-Bote, by contrast, encrypts everything except for the recipient's Email Destination. It also has the ability to send an email through several relays (similar to Mixmaster), so nobody can find out who is sending email to who.

How does it compare to Susimail?
I2P-Bote is better because it has a higher version number. Just kidding.
I2P-Bote offers more privacy, but Susimail has some features I2P-Bote doesn't have yet (see below), and Susimail is more bandwidth-efficient because it doesn't store emails redundantly.

How do I create an email account?
I2P-Bote calls them Email Identities. You can create one in the I2P-Bote web interface under the "Identities" link. The reason why it's not called an account is that there is no provider like GMail or GMX. You alone hold the (cryptographic) keys to the Email Identity.
When you create an Email Identity, I2P-Bote generates a string of numbers and letters called an Email Destination. This is the address you can be reached at.
Example: `wsq-8u5bTWbaOsrS0JuXRKL-RsbTkckV4W7u2mIu0Yrlfetixq1F~03CArnvbd6tDWwjPHYEuoKyWqwxplSdix`

What's an Email Destination? What about email addresses?
Email destinations are between 86 and 512 characters long, depending on the type of encryption. Support for easy-to-remember, user-chosen addresses is planned for the near future.

Which encryption type is best?
256-bit ECC produces short and handy Email Destinations, and it is considered stronger than 2048-bit ElGamal.
512-bit ECC is stronger than 256-bit ECC, but it makes Email Destinations longer.
2048-bit ElGamal produces even longer Email Destinations, and it is the cryptographically weakest of the three options. However, ElGamal is better researched than ECC, which makes it less likely that there is an unknown weakness in ElGamal than in ECC.

What algorithms are used for symmetric encryption, and for hashing?
AES-256 in CBC mode and SHA-256.

Can I send attachments?
Yes, attachments are supported as of release 0.2.5.

Are there any anti-spam measures?
I2P-Bote does no active spam filtering, but the fact that mass emails have to be sent individually should discourage spammers. Another line of defense is HashCash which is supported at the protocol level and may be implemented in a future version if spam becomes a problem.

How long are emails kept around?
Emails are available for 100 days after they have been sent. Emails that have not been downloaded by then are deleted. Emails you have received stay on your local machine until you delete them.

When do Email Identities expire?
Never.

Can I send email to, and receive email from normal internet email servers?
No, but this is being worked on.

Can I use an email program like Thunderbird?
No, but it is on the roadmap.

How do I migrate my settings and data to another computer, or back them up?
I2P-Bote stores all email and other data in the `i2pbote` folder. On Windows, that folder can be found at `%APPDATA%\I2P\i2pbote`; on Linux, it is `$HOME/.i2p/i2pbote`.
To back up or migrate everything, just copy the whole `i2pbote` folder.
If you are only interested in your Email Identities, copy the file `identities.txt`. For the address book, copy `addressBook.txt`.

What languages are available?
English, German, and Russian.

How can I help translate I2P-Bote into my language?
Translations are done the same way as the rest of I2P. If you would like to help and have questions, please contact the author.

How does it work on a technical level?
Have a look at the file `doc/techdoc.txt` in the source code.

What are some other ways I can help?

- Use I2P-Bote and give feedback
- Write a user's guide or improve the technical documentation
- Add features or fix bugs (contact the author first)

CSS: David Herreman

XHTML - CSS