17 May 2017

Message Log

Overview and Use

Purpose

Establishes a secure and purposely ambiguous communications pathway between any two individuals, so that they may communicate with anonymity exceeding that of email. The site is completely open, minimalist and simple to use. The site has little to hide, so it can reveal almost nothing if successfully attacked. What you see is about all you will get.

Functional Overview

This site allows you to anonymously post a message into a common public file (the Log). It also allows you or anyone to read that Log in its entirety.

The site uses SSL for communications security. An eavesdropper is prevented from reading any data as it passes across the system. (SSL security is commonly used for passing credit card info over the web.)

This site has amnesia. It does not inquire, store, or indicate any user's identity or IP address.

This site has no knowledge of, and provides no message security. Message security is entirely up to the sender/recipient pair (end-to-end encryption). Once posted, a message is available for all to read for 48 hours. Where message security is unimportant, plain text may be used.

User Instructions

Upon entry into the site, you are at the main “Message Log” screen. From here, you can:

1. Read the Log

Click the "Read All Messages" button. The entirety of the Message Log contents, that is, every message posted into the Log during the last 48 hours, will be pushed onto your screen.

2. Post a message to the Log

Enter your message, then enter password and click the "Post Message" button. A confirmation screen will verify the message was accepted and placed into the Log. The confirmation displays three items:

- the assigned message number,
- the posting date-time, and
- a reminder that the message will be deleted from the system in 48 hours.

An incorrect password invokes, an "Entry Denied" warning, and no message is posted.

Message Content for Posting

To promote interesting uses, there are very few limits on the message. At this time, there are no limits on message size. (That could be a fatal flaw!) The screen for message entry is 81 columns wide. Continuing past that limit will wrap the screen, but it does not wrap the data posted to the Log. (The site adds nothing to the posted message - encryption programs are generally intolerant of ciphertext

changes.) If 81 display columns prove limiting, it can be expanded in a follow-up revision. (You must use an occasional carriage-return or your entire Log entry will be on just one very-long line!)

You are free to directly type your message into the message box on the screen or cut-and-paste it from elsewhere (like from Word, Notepad, or an encryption program).

Message Log Format (Read All Messages)

At the top of the page, preceding the messages is:

- the present date-time,
- a reminder that messages older than 48 hours old have been deleted, and
- the last message number deleted (all prior messages will have been deleted).

Following this preamble is every message posted within the last 48 hours. Each message is preceded by its message number, and posting date-time. To facilitate a copy/paste into a decryption program, the message is contained within angle brackets. That is, the message starts in column 1 on the line immediately following the start-of-message indicator, ">>". The "end-of-message" indicator, "<<+", is on the line immediately after the last character of the message. (Any blank lines seen between the start-of-message and end-of-message indicators are part of the contained message.)

Each message is separated by one blank line.

Example of Log Format:

Wed, 3-MAY-2017, 19:02:45 z.
Messages auto-delete after 48 hours.
Message 1493665165 and prior deleted.

msg:1493744122:
Tue, 2-MAY-2017, 16:55:22 z.
>>
This is the first example message that
I recently submitted. It obviously is not
encrypted.
<<+

msg:1493743444:
Tue, 2-MAY-2017, 16:44:04 z.
>>
This is my second and last example message. It,
too, is not encrypted.
<<+

17 May 2017

Security Analysis

Comms Security: All communications with the Message Log is via Secure Socket Layer (SSL), an asymmetric cipher negotiated between the website and your browser. (Note the "https:" and the padlock symbol at the top of your browser). This secure pathway hinders an eavesdropper from reading the data as it is passed, in either direction, between the website and the user. The observer may only infer info from the quantity of bytes passed.

Message Security: The users are responsible for their own message security. No message security is provided by the site, nor would you want it to. Hence, a successful attack can never reveal the message content. Once posted to the Log, a message may be read by anyone.

Each sender/recipient pair (end-to-end encryption) must agree upon and coordinate an encryption method based upon their required level of message security. This could be an asymmetric cipher (public-private key pair), requiring no aforehand key distribution, or they could use a symmetric key cipher requiring the sender and recipient to meet privately to exchange keys. The method is entirely up to each communicating pair of users and may substantially differ from other user pairs. Letting the users determine their own encryption method adds flexibility and removes the middleman (the site) from the message security equation.

If message security is unimportant, a plaintext message may be posted, still maintaining anonymity.

Password: The password used to enter a message is common for all users and serves only to reduce the probability of a third party overloading the system, creating a denial of service for legitimate users. Otherwise, no individual password is used as it may lead to revealing the user's identity.

Addressee: There are no To/From headings. The site does not inherently know, therefore can never reveal the sender nor the recipient. It is essential that the sender and recipient agree upon a method of recognizing each other's messages. Using this pre-arranged method is the only method a recipient can recognize a message is for them. When a user reads the Message Log, all messages in the log are received, whether destined to the user or not. Hence, an observer cannot determine whether any, all, or no messages are addressed to the reader.

One suggestion is to note the assigned message number and pass that number to the recipient, via some unrelated method, like via text message. The recipient then gets a "heads-up" that he should go to the Log and find his message. Otherwise, an agreed upon message line could encode an addressee. Where security is utmost and no passing of a message number is possible, the recipient is implied as only he possesses the knowledge to decrypt the message.

Identity by IP: Realize that a real-time observer can always know (by IP address) who and when a user is connected with the Message Log site. The observer may infer (by the quantity of data sent) that a message was sent, but can never be sure that a message was ever delivered. If the identity of a sender and/or recipient must absolutely be maintained, connect your iPad to the WiFi at a different location.

Message Deletion: No one, including the recipient, is allowed to delete a message. If a recipient could delete a message after reading, an observer might correctly infer that the message was received, and determine which message went to whom. Messages over 48 hours old are automatically deleted by the site.