Hermetic Systems releases a program for secure end-to-end email encryption

Released on: April 29, 2013, 7:01 am
Author: **Hermetic Systems**
Industry: <u>Software</u>

April 29, 2013, 7:01 am -- /<u>EPR NETWORK</u>/ -- Despite substantiated reports that at least one major US telephone service provider gave the National Security Agency full access to its customers' phone calls, and shunted its customers' internet traffic to data-mining equipment installed in a secret room in its San Francisco switching center, most Americans still transmit their email in plaintext, allowing it to be scanned by data-sniffers. (The NSA was ordered by a court to stop, but who knows if they complied?) This may be because most Americans don't give much thought to the possibility that their email could be the subject of eavesdropping, or it could be because for some reason it doesn't worry them, or it could be because encrypting email has in the past been a somewhat tricky practice to get right (so was deemed not worth the effort).

There are several reasons why email encryption can be difficult, or insecure: Some systems are quite secure but require an elaborate procedure before email can be sent to (and read by) another person. Messages scanned in transit can in the case of some systems reveal that encrypted information is present, thus alerting an eavesdropper to something to look for. Some systems encrypt a message only after it is uploaded

to a server, with the message (in plaintext) being vulnerable to interception between the user's PC and the server.

Hermetic Systems has release software for email encryption which involves none of these difficulties. But why would you want to use it? For correspondence with your family you probably don't need to. But, for example, suppose you are collaborating with others in a project which requires an exchange of confidential information, which competitors might like to get their hands on. You might be wanting to transmit Excel files containing sensitive financial data, or images with blueprints for a new design.

The new software, entitled 'Email Encryption End-to-End', uses an encryption method in which the key used for encryption is the same as the key used for decryption, so your correspondent(s) must know the key you used to encrypt a message. This can be transmitted more-or-less securely, especially if you can meet your correspondent(s) in person. Assuming this can be accomplished, the actual sending and receiving of encrypted messages is quite simple. You run the program (on your PC), compose a message of up to 60 KB in size (or upload it to the program from a file) and specify an encryption key, then hit the 'Encrypt' button. This creates a ciphertext file (which you can name as anything you want), and to send it to a correspondent you simply attach it to an ordinary email message. The ciphertext can masquerade as an image file or as a file using some obscure file format, so there's no indication that encryption is being used.

You correspondent receives the ordinary email, saves the attached (ciphertext) file, runs the software, tells it where to find the file, specifies the encryption (now decryption) key, and hits the 'Decrypt' button, whereupon the message appears.

Moreover, 'Email Encryption End-to-End' allows you to send, in addition to a text message, a file of any type and up to 1 MB in size. The text message and the file are then combined and encrypted together to produce the ciphertext file. This allows

you to send an MS Word file, an Excel file, an image file, etc., in addition to the text message.

The program has an introductory price of US$29.75. A multi-user license is also available (at a discount) for up to 10 users. Such a license is useful for a group of colleagues working together on a single project. A multi-user license requires only a single email address, that of the purchaser of the license, and the email addresses of the purchaser's email correspondent(s) are not needed.

A trial version can be freely downloaded from the user manual page at http://www.hermetic.ch/eee/eee.htm. This is a 14-day trial with which only one key ('abcd efgh ijkl mnop') can be used for encryption, so it allows testing but (since the key is public knowledge) cannot be used for secure email encryption.

Contact Details: Hermetic Systems
support@hermetic.ch
http://www.hermetic.ch/
Schützenmattstrasse 5
CH-4051 Basel
Switzerland

~~~~~