Email Encryption End-to-End: How to Prevent the NSA from Reading Your Confidential Email Messages

Released on: June 18, 2013, 11:03 am
Author: **Hermetic Systems**
Industry: Software

June 18, 2013, 11:03 am -- /EPR NETWORK/ -- Anyone who has not spent the last two weeks meditating in a cave will have heard about PRISM, the program of the National Security Agency (NSA) to spy on anyone they wish using the internet services provided by Microsoft (beginning in September 2007), Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL and Apple. These are all mentioned in one of the slides of a 41-slide top-secret Power Point presentation (an overview apparently intended to train intelligence operatives on the capabilities of the program) which was leaked by NSA whistleblower Edward Snowden to the Guardian (UK), which newspaper revealed the astonishing details on June 6. The document claims "collection directly from the servers" of major US ISPs.

The existence of PRISM was confirmed by the U.S. Director of National Intelligence (James Clapper) in a press release on the same day, stating that the program was authorized by Section 702 of the Foreign Intelligence Surveillance Act (FISA), and claiming that it is intended only to facilitate the acquisition of foreign intelligence information concerning non-U.S. persons located outside the United States.

However, according to the Guardian, "The program facilitates extensive, in-depth surveillance on live communications and stored information. The [FISA] law allows for the targeting of any customers of participating firms who live outside the US, or those Americans

whose communications include people outside the US. It also opens the possibility of communications made entirely within the US being collected without warrants." Section 702 of FISA says that senior officials of the U.S. administration can authorize the surveillance of any American provided that the request officially targets a foreigner. This allows "legal" access to all private information concerning anyone (whether or not they reside in the US) "associated with" the "foreign suspect".

Private information, of course, includes the content of email messages, and those that the NSA sucks up are stored for years (forever?) in the huge NSA data banks. The standard claim of government defenders of invasive surveillence is: "If you have nothing to hide then you have nothing to worry about." There are several answers to this.

Firstly, if you work with proprietary or confidential information, such as business plans, software code, financial statements, etc., then you may very well wish to hide this from others who might make use of it to your disadvantage (and if you work for a company which owns this information then your failure to hide it from your company's competitors may lead to your dismissal).

Secondly, as Edward Snowden said in an interview with the Guardian: "... you don't have to have done anything wrong. You simply have to eventually fall under suspicion from somebody even by a wrong [phone] call. And then they can use this [PRISM] system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with. And attack you on that basis to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer."

So can you do anything about this? It's just possible that massive public outrage at the development of a total surveillance state might cause PRISM to be shut down. But don't hold your breath. You can, however, do something to prevent the NSA from reading your confidential email messages. You could use public key cryptography in some form. This requires the creation of a 'private' key and a 'public' key, and anyone who wishes to send you an encrypted message has to know your public key (and you then decrypt the message using your private key). This is fine, but it's a bit complicated and requires considerable attention to detail, so is really only suitable for the tech-savvy. There is an easier way to keep your messages and data from the NSA's prying eyes (just in case you are a person of interest to them).

Hermetic Systems publishes Windows software called "Email Encryption End-to-End" which, in brief, allows you to create an encrypted file containing both a text message and a separate file of any type (such as a ZIP file). You can then attach this encrypted file to an ordinary email message, send it, and the recipient can recover your text message and the file using the same software. Your message and file remain encrypted from start to finish, frustrating any attempt by the NSA to read them.

This software is easy to use and no technical knowledge (beyond the ordinary ability to run a Windows program and to send and receive email) is needed, and you can still use the same email client as you do now (provided that it allows attachments to messages).

Suppose your company wishes to send you somewhere to negotiate a business deal with some other company. They will want to know the details of the deal you make with that company as soon as you have concluded the negotiation, so you are to write it up on your laptop as a Word document (and maybe a few Excel spreadsheets) and send it by email. But your company's competitors would dearly like to know the details of the deal you make, so you are instructed to send the document (and spreadsheets) in encrypted form. Before leaving, you are given a phrase to use as the encryption key. After several days negotiation you reach a deal, and prepare your report.

Now suppose also that a year ago someone who works at a shady payment processing service phoned you by mistake; this service was subsequently shut down for alleged money-laundering, but in the meantime that phone call got you placed on a list of "known associates of suspected money-launderer", and subject to surveillance under the PRISM program. Of course, you were not informed. But since you and your company know that transmission of unencrypted data across the internet allows "sniffers" to pick out selected messages, and that certain competitors would dearly like to know the details of the deal you just negotiated (and, unknown to you, certain people who work for NSA might also profit from knowing those details) you are about to send your report by means of encrypted email. Here's how to do it:

You take all the confidential material (Word documents, Excel files, graphics images, etc.), and put them into a ZIP file. Without being online, you run the "Email Encryption End-to-End" (EEE) software and this allows you to (a) compose a text message which summarizes the outcome of the negotiation and mentions what's in the ZIP file, (b) tell EEE the location of the ZIP file, (c) enter the phrase which your

company gave you to use as the encryption key, and (d) tell EEE the location and name of a file in which it will write its output -- the 'ciphertext file. The ciphertext file can have any name, but let's say 'chess.pcx'. You then hit the 'Encrypt' button and EEE encrypts your text message together with the ZIP file and writes the encrypted data to the ciphertext file. Now you go online and bring up your usual webmail client. You compose some pedestrian message, such as, "Chess tournament went well; got 2nd prize; here's a picture of the prize winners." You then attach the ciphertext file to the message and send it off to your company.

The person at your company meant to receive it then saves the attached file someplace, then runs EEE and (a) enters the agreed-upon phrase for the encryption key and (b) tells EEE where to find the ciphertext file. They then hit the 'Decrypt' button and EEE (a) displays your text message mentioning what's in the ZIP file and (b) asks for the location of a folder in which to write it. After it does this, the recipient can then unzip the ZIP file to recover the documents that you sent.

NSA may have sucked up and stored your 'outer' email message in its data bank, but this will appear to be just some message about a chess tournament with an attached 'pcx' file referred to in the message as a picture. No graphics software will be able to display it (because it is not a graphics file), and no ZIP program will be able to unzip it (because it is not a ZIP file), and in fact it can't be read at all, except by someone using the EEE software and knowing the phrase used to encrypt the data. Your confidential data has been transmitted securely in encrypted form from 'end to end'.

Finally, if there is some chance that your laptop might fall into the wrong hands before your return, you can (after your company has confirmed receipt of your report) delete (or better, securely delete) the ciphertext file which was created by EEE (and perhaps even uninstall the EEE software itself), since the details of your negotiation are now safely in the hands of your company.

Further information about the "Email Encryption End-to-End" software (which is bilingual, English/German) including prices for a single-user license and for a multiple-user license, plus a link to download a trial version, is on the Hermetic Systems website at:http://www.hermetic.ch/eee/eee.htm

Contact Details: Hermetic Systems

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

~~~~~
~~~~~