



A focus on secure communication: Why you should sign and encrypt your emails

 The article was obtained at the following URL: <http://www.kfwebs.net/articles/article/21>
 The article might be distributed further as long as it is provided as it is, with the credits stated.
 The Article was written and first published by KF Webs, at <http://www.kfwebs.net>
 #####

Say Alice sent an email to her executive, Bob, claiming to be Charlie. She included some comments that made Bob react against Charlie. Charlie got a reprimand or lost his job. This is a situation that could be avoided by integrating digital signatures in the solution.
 Added: 2005-08-11 14:13:10 - Modified: 2005-11-09 08:53:20 - Level: Beginner

Why you should sign and encrypt your emails

Digital signatures

Digital signatures provide a means to verify that the sender is whom he or she claims to be. It is very easy to forge from-addresses, something you might have noticed related to viruses spreading and spam coming into your mailbox from senders you are certain didn't send it.

Say Alice sent an email to her executive, Bob, claiming to be Charlie. She included some comments that made Bob react against Charlie. Charlie got a reprimand or lost his job. This is a situation that could be avoided by integrating digital signatures in the solution.

Encryption

Lets start with a question; when you send a letter, do you fold it in an envelope? Why don't you put all your personal data on a postcard? You do this to protect your privacy. Emails are sent in plain text over the internet, usually through several relays before reaching the end goal. Without encryption anyone can read the email on the way.

The European Parliament conducted an investigation against the Echelon-system in a periode between 1999 and 2004, the final report might be read at <http://cryptome.org/echelon-ep-fin.htm>. But what is this echelon thing? Quoting: <http://fly.hiwaay.net/~pspoole/echelon.html>

In the greatest surveillance effort ever established, the US National Security Agency (NSA) has created a global spy system, codename ECHELON, which captures and analyzes virtually every phone call, fax, email and telex message sent anywhere in the world. ECHELON is controlled by the NSA and is operated in conjunction with the Government Communications Head Quarters (GCHQ) of England, the Communications Security Establishment (CSE) of Canada, the Australian Defense Security Directorate (DSD), and the General Communications Security Bureau (GCSB) of New Zealand. These organizations are bound together

under a secret 1948 agreement, UKUSA, whose terms and text remain under wraps even today.

The ECHELON system is fairly simple in design: position intercept stations all over the world to capture all satellite, microwave, cellular and fiber-optic communications traffic, and then process this information through the massive computer capabilities of the NSA, including advanced voice recognition and optical character recognition (OCR) programs, and look for code words or phrases (known as the ECHELON "Dictionary") that will prompt the computers to flag the message for recording and transcribing for future analysis. Intelligence analysts at each of the respective "listening stations" maintain separate keyword lists for them to analyze any conversation or document flagged by the system, which is then forwarded to the respective intelligence agency headquarters that requested the intercept.

Now, many will probably say that its not a problem that the government surveillance them, as they have nothing to hide. If you just had this thought, please read the final report. Chapter 10.7. Published cases include some reading material for you. One case worth to mention is one of **Airbus versus Boing** in 1994. Where NSA obtained "*Information on an order for aircraft concluded between Airbus and the Saudi Arabian national airline*" using the means of "*Interception of faxes and telephone calls between the negotiating parties*" with the goal of "*Forwarding of information to Airbus's US competitors, Boeing and McDonnell-Douglas*", which resulted in "*The Americans won the contract (US\$ 6 bn)*"

S/MIME

S/MIME rely around the use of a Central Authority, such as Verisign to provide authentication for a user. The main advantage is that S/MIME seem to be integrated in several mail clients, whereby pgp often require a plugin.

OpenPGP

OpenPGP, or PGP itself evolve around a Web Of Trust. This mean that OpenPGP depend on users verifying other users and digitally signing eachothers public keys as a token of authentication. More information about OpenPGP, often refered to as just PGP (which can be confused with the application Pretty Good Privacy, that is the basis of the OpenPGP standard), can be found at <http://en.wikipedia.org/wiki/Openpgp>

On the technical note: OpenPGP and PGP/MIME spesifications are found in Internet Engineering Task Force's Request For Comment (IETF RFC) 2440 and 3156 available from <http://www.ietf.org>, the OpenPGP Alliance can be found at <http://www.openpgp.org/>

Why focus on OpenPGP?

The OpenPGP approach might seem rather hard. Why go through the process of signing other users key when you can just have some third party (exempli gratia Verisign) to do it for you? One of the answers to this is trust. You might not trust in that third party required using S/MIME enough to authenticate the users you communicate with. Another answer is conveniense. If you are to communicate with a user you usually meet up in front, and can easily exchange the needed information in front, whereby you'd have to generate a

certificate, a certificate signing request and await processing from a central authority otherwise.

Another reason is the price, for personal use you can get a free certificate from e.g. Thawte, but as soon as you want to use it in relation to anything commercial you'll have to pay for each one. The certificate is time-limited and you have no control over the keys generated.

Using OpenPGP

To get a list of applications that support OpenPGP and eventually corresponding plugins, visit <http://www.bretschneider.net.de/tips/secmua.html>. To mention some; [Mozilla Thunderbird](#), using [Enigmail](#) and Evolution support PGP/MIME (somewhat limited as discussed in <http://www.kfwebs.net/articles/article/19>)

Practical information exchange

I usually carry the details necessary to exchange key information with me in my wallet in case I meet someone who potentially will communicate securely with me.

```
sub 4096/60B0B9508 created: 2005-02-21 expires: never usage: C5
Primary key fingerprint: 6DF1 73BE C945 0DA6 7A5E 6197 16D0 C7BD 8808 9508
sub -4096g/8888F803 created: 2005-02-21 expires: 2005-12-31 usage: E
(1) Kristian Fikerstrand <kristian.fikerstrand@kfwebs.net>
(2) Kristian Fikerstrand <kf@kfwebs.net>
(3) [jpeg image of size 3387]
```

Signing policy and key info at <http://www.kfwebs.net/pgp>



Kristian Fikerstrand date

It provide the key size and type, the key identification number, the date it was created, the usage for the key and the fingerprint of the primary key, as well as the different user identification strings attached to the key, the picture ID, as well as fields for me to enter the date and my signature.

Now, the most observative of you might notice that it list two, and not one key id and size. In my case a primary key of ID 0x6B0B9508 used for Cerification and Signing, and a subkey with the usage of Encryption. The reason for this is, beside technical reasons to use different keys for signatures and encryption, that you will usually want the signing key to last for a while (or in my case forever) while you might want to change the encryption key once in a while.

I usually change the encryption key once a year to show that my key is active. One reason for this is that you can't encrypt messages to keys which are expired, and you will therefore have to refresh the key, either by downloading it from my website or by refreshing it from a PGP Keyserver. If my key has been compromised in any way, I will by that time have revoked it, and you will stop sending emails that might be read by others. Of course once a year might be too seldom, so I suggest people refresh their keyring once in a while to get updates.



Related articles:

[A focus on secure communication: kggg](http://www.kfwebs.net/articles/article/20)[http://www.kfwebs.net/articles/article/20] ([Focus on secure communication](#))

[A focus on secure communication: Mozilla Thunderbird and Enigmail](http://www.kfwebs.net/articles/article/22)[http://www.kfwebs.net/articles/article/22] ([Focus on secure communication](#))

[A focus on secure communication: Evolution](http://www.kfwebs.net/articles/article/19)[http://www.kfwebs.net/articles/article/19] ([Focus on secure communication](#))