

E-Mail Security for the 21st Century

E-mail has inherently been an unsecured method of communicating since its inception. While today e-mail is a frequently used and convenient method of exchanging information, such usage was not planned for in the technology's beginning. The basic principles of e-mail were established more than thirty years ago when the Internet, then called ARPANET, was an emerging technology. Trust was a basic principle of the Internet back then. Universities, military, and governmental facilities were the only users of the Internet and everyone knew everyone else. Back then there wasn't a need for authentication of who actually sent the message because only a limited number of people could gain access to the networks over which the messages were traveling. When networks began connecting to each other, e-mail security became more important. Users realized that they needed verification of who was sending the message to make sure no one has changed the message during transit, and, in some cases, they realized they needed to secure that information against prying eyes.

By the mid 1990s, e-mail security became a needed addition to the messaging people already knew. Two protocols emerged as standards: Pretty Good Protection (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME). Both offered digital signatures¹ which added the capabilities of authentication, non-repudiation, and data integrity. Message encryption added the capabilities of confidentiality and data integrity. For the user this helped ensure two things: First, that only the intended recipient can read the message. Second, that a person reading a message can be assured of the identity of the sender.

History

PGP

When the Internet went public in the mid-1970sⁱⁱ, it opened up for anybody to have access. That open access made all users more vulnerable because of the possibility that some users might have bad intentions. Many vulnerabilities had not been discovered at the beginning, but it was only a matter of time.

In 1982 a standard was created that standardized the way we send e-mailⁱⁱⁱ. SMTP, or Simple Mail Transfer Protocol, was developed by Jonathan Postel who saw it necessary to create a system that would provide reliability for sending messages over slow and unreliable network connections. A large problem with SMTP was that it did not require authentication to be able to send messages^{iv}. Thus people could send messages without the server checking to make sure they were who they said they were. This became a problem that still exists today.

Along with the authentication problem came the privacy problem. Again, trust was a big part of messages making it from the sender to the receiver without anyone reading or changing the message while it was making its way along through the network. Then, in April of 1991, something happened that made quite a few people sit up and take notice. A non-binding resolution was added to Bill 266 in the US Senate that read like this:

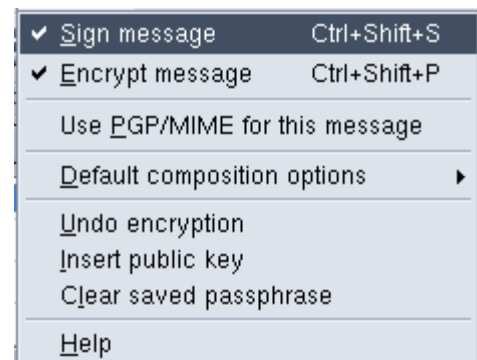


Illustration 1: Screen shot of PGP options box

"It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the Government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law."

This made Philip Zimmermann work hard to create his software that would allow the general public the ability to protect themselves. He called it Pretty Good Privacy or PGP which was based on the RSA public-key protocol^v. For the first time, the general public had access to a secure means of communication without the fear of government oversight. This could be the difference between life and death in some countries where the government watches all network traffic coming into the country, leaving the country, and going within the country.

While PGP is being used by corporations, educational facilities, and the government to protect their sensitive information, a new version of PGP was being created that would help push this technology out to the public. GnuPG was developed by Werner Koch in 1999^{vi}. GnuPG is an open source version of PGP that supports the same types of encryption but is available for free. This was a big step in pushing this technology out to the people. It can be downloaded for free and allows users to encrypt and digitally sign their messages.

PGP uses public key infrastructure (PKI) for signing and encrypting messages. When an encrypted e-mail is sent the message is encrypted using the sender's private key and the recipient's public key. The recipient then uses his private key and the sender's public key to decrypt the message. All private keys should be protected with a strong passphrase and private keys should be protected against disclosure.

If the private key was ever known then all encrypted messages could be read. Further, messages could be signed and encrypted by the person who has the private key and not the owner, which would negate the use of the key. Superseding keys on a regular basis will help protect the integrity of your signed and encrypted messages^{vii}.

S/MIME

At nearly the same time, a new security protocol came out called S/MIME (Secure/Multipurpose Internet Mail Extensions). S/MIME was fast becoming a standard by the Internet Engineering Task Force (IETF) during the late 1990s. Microsoft had a hand in version three of the S/MIME protocol having wide public acceptance by including support for this in the manufacturer's Outlook, Outlook Express, and Exchange programs. Today, most e-mail client software packages work nearly seamlessly with S/MIME and thus works behind the scenes to most users. It allows both email encryption and authentication. Both use asymmetric encryption, public-key technologies.^{viii}

S/MIME version 2 is not an IETF standard due to security risks associated with using smaller keys than what is considered breakable. Version 3, however, has been awarded an IETF standard and is the only version of S/MIME that should be used.^{ix}

Choosing a Solution

There are a number of options available for messaging using either PGP or S/MIME. Each have pros and cons, but all provide a degree of security for the user. Users can decide which option works best for

them based on pricing, the e-mail client they want to use and the ease of usage.


PGP

Today, the PGP, or Pretty Good Protection, software requires a purchase from the PGP Corporation. Different versions of the software are available^x for different purposes including e-mail, total computer, and key management for enterprise solutions. PGP is also available for BlackBerry^{xi} hand held devices as well which supports enterprise solutions that companies may have implemented for company-wide encryption solutions. While PGP is an excellent solution for businesses and companies, it could be an expensive investment for personal use.

GnuPG and OpenPGP

GNU Privacy Guard (GnuPG) is an open source version of PGP and can be downloaded for free from GnePG.org. GnuPG is the encryption back-end program for some additional open source software that completes the solution. GnuPG provides file encryption and signing capabilities but OpenPGP provides the front-end solution to work with e-mail client software to implement signing and encryption capabilities.

Enigmail

Enigmail is a Mozilla project^{xii} that uses OpenPGP to add PGP capabilities to Thunderbird and  Seamonkey, both e-mail clients. Enigmail allows users to sign and encrypt messages and attachments and verify signed and encrypted messages that have been received. Enigmail uses OpenPGP Key Manager^{xiii} to manage stored public and private keys

which provides a stable, powerful, and common key management system. Enigmail is available as an extension to Thunderbird.

S/MIME

S/MIME certificates are usually assigned by a trusted source and thus are usually issued by dedicated security companies. Thawte is one of those companies that issues S/MIME certificates, as well as SSL certificates, but does something that most companies don't.



Thawte issues personal S/MIME certificates for free and even has its own web of trust that establishes rules for verification of the owner of the certificate. This is important as you must trust the procedure of verification of the owner or you wouldn't be able to trust the signed documents that you receive. There are other companies that provide S/MIME certificates but are more driven to the business world versus the public and thus cost more money.

Because the S/MIME standard is used by so many different clients, implementation of this solution is rather easy. Most e-mail clients have settings for S/MIME security built-in. With the settings built-in

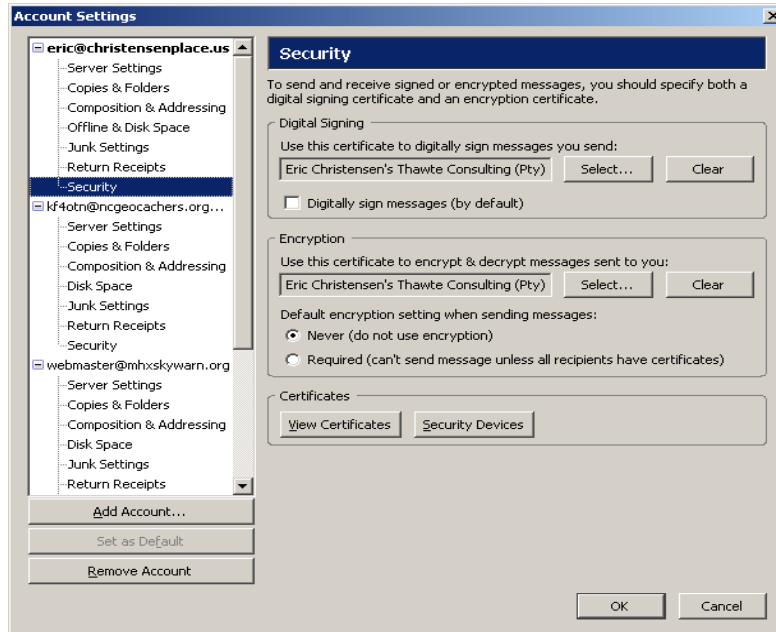


Illustration 2: Screen shot from Thunderbird 2.0 showing security account settings.

there is no need for additional software. While this is a big plus, there are some drawbacks from using S/MIME over PGP.

The Down Side of PGP and S/MIME

S/MIME

S/MIME messages present an unusual problem for users that do not use a client that is designed to handle S/MIME messages. These programs actually present the signature as an attached file which can confuse the recipient and can cause some programs to flag the message as suspicious. Many users of “webmail” clients experience this problem and many users fear these attachments as being viruses. This can be counter productive to the desired outcome.

PGP

With PGP, and its variants, having been out on the street for over ten years an amazingly low number of people actually use this solution. This could be a result of having to set up and use an additional piece of software or because people just don't see the necessity of securing their communications. Also, a non-user might be confused by receiving a signed message from a user of PGP because of the injection of the PGP signature at the end of the message (see Illustration 3 below). This additional information does not harm non-users in any way.

```
<http://www.us-cert.gov/legal.html>
This document can also be found at
<http://www.us-cert.gov/cas/tips/ST04-007.html>

For instructions on subscribing to or unsubscribing from this
mailing list, visit <http://www.us-cert.gov/cas/signup.html>.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (GNU/Linux)

iQEVAwUBRhOsJexOF3G+ig+rAQJjCQgAkqLoMWZIwfjjLTpOhUMuhmpawzt+Nfi6
cNTXjHr8JBPUjMccKR9Z7By2reiNOtCfyOzDOZ1K1DLm2gYVoMIRZW/T4LOPM11T
TWI8a3hWxVBh6mpEvTbZs4meJ/b0e/cZn1ZlxDj1cHoNFH1UX4gBWHxB7BhAhi/B
Jwenvqe3Cns9k3dNJ0y94Q19YWOaMznrtY9Vs3uofiMYSDIRuLF/mygtbHs7xUzW
4wRTjrao22Obnbn5J62R/FaFb1aCNacAZUWwK6eQvgPlakCZWYFRPdHJyqFOXoay
ADVb/EdDpNmMyEyLvMng50aPk6HRtZV1Ishug7/rwIcX//4ViE5gnQ==
=6mwa
-----END PGP SIGNATURE-----
```

Illustration 3: Received e-mail with a PGP Signature

Summary

The Internet has changed greatly over the years, making security more important today, particularly for users wishing to transmit sensitive information. PGP and S/MIME will provide users with protection when sending messages over networks and over the Internet. Depending on which standard you wish

to embrace your setup may vary. But the end result will always be the same: you will be more secure and your information will be less at risk to interception.

The author, Eric H Christensen, is an information technology professional with a government agency and can be reached at eric@christensenplace.us.

- i Microsoft TechNet, Understanding S/MIME <http://technet.microsoft.com/en-us/library/02deb7c5-89d4-4e15-9300-5fc355ea83a4.aspx> 29Mar07
- ii History of the Internet <http://www.virtualschool.edu/mon/Internet/CerfHowInternetCame2B.html>
- iii History of SMTP http://www.circleid.com/posts/history_of_smtp/
- iv Net History, The history of email <http://www.nethistory.info/History%20of%20the%20Internet/email.html> 27Mar07
- v Pretty Good Privacy http://www.livinginternet.com/i/is_crypt_pgp.htm 27Mar07
- vi GNU Privacy Guard, History http://en.allexperts.com/e/g/gn/gnu_privacy_guard.htm 27Mar07
- vii GnuPG FAQ, [http://www.gnupg.org/\(en\)/documentation/faqs.html](http://www.gnupg.org/(en)/documentation/faqs.html)
- viii RSA, SMIME, <http://www.rsa.com/glossary/?id=1051>
- ix Internet Mail Consortium, S/MIME and OpenPGP, <http://www.imc.org/smime-pgpmime.html>
- x PGP Encryption Products <http://www.pgp.com/products/index.html>
- xi PGP BlackBerry Solution http://www.pgp.com/products/pgp_support_package_for_bb/index.html
- xii Enigmail Project Page <http://enigmail.mozdev.org/>
- xiii Enigmail OpenPGP Key Manager <http://enigmail.mozdev.org/keyman.html>