Using PGP to Verify Digital Signatures

Shawn Hernan and Linda Pesante
CERT® Coordination Center

PGP stands for Pretty Good Privacy. It is a computer program that uses mathematical algorithms to encrypt files and protect them from unauthorized access. It is also used to digitally sign and verify documents. Versions of the PGP program are available for most popular computer operating systems—Microsoft Windows, MacOS, and UNIX, to name a few.

Because most of our constituents receive documents that are signed with the CERT/CC PGP key, we focus on the second use. In this paper, we provide some background information about PGP and explain how to check signatures for validity.

A PGP signature appears as a block of seemingly random letters and numbers at the end of the text. A valid digital signature tells the reader of the document that it was written by the owner of the PGP key and the text hasn't been changed in any way since it was signed.

A publicized example, illustrating the need for verification of documents, arose at a university. A student forged an email message to a class in the name of the instructor, claiming that there had been a death in the instructor's family and the final exam was postponed. As a result, most of the class members did not show up for the final.

PGP keys

PGP is based on *keys*, a public key and a private key. For example, the CERT/CC has a *private key* for signing documents. We protect our private key carefully, and only authorized members of the CERT/CC staff have the password that allows them to use the key.

Each private key is paired with a *public key* that is available to anyone. The CERT/CC key can be downloaded from our web site as well as from other locations (called *key servers*) that collect public keys from many organizations. Details and a link to our PGP key are on the CERT/CC web site at https://www.cert.org/contact_cert/encryptmail.html.

Keys are bundled with information about the key, such as the name of the owner and the date the key was generated. The bundles of information containing the key are called *key certificates.* Many key certificates include signatures of individuals or groups that help attest to the veracity of the key (there's more on these signatures in the *Web of trust* section). Key certificates are stored in files called key rings. Your private key ring holds your private key, and your public key ring holds the public keys of everyone whose sends you documents signed or encrypted with PGP

Web of trust

A key (pun intentional) concept for PGP is that of a web of trust. Owners of PGP keys get others people's signatures on their key, enabling you to infer a level of confidence that the signed key belongs to the person named in the key's *userid* section. For example, let's say that you receive a message signed with the key of John Doe, an individual you don't know. If John's PGP key contains a signature of a person or group you do know and trust, you gain trust in the identity of the stranger by virtue of your mutual, trusted acquaintance.

Let's say that John Doe's key is signed by Rich Pethia of the CERT/CC and ISA or Dave McCurdy of the Electronic Industries Alliance and ISA. You trust them because you know them, either personally or by reputation, and are confident that they are trustworthy, ethical individuals. Moreover, you have validated their keys—verified that the key claimed to be theirs is indeed their own key, a critical step for building trust. (If you see a signature that claims to belong to someone you trust, you should not believe it until you have checked to see if the signature is valid.) Then, when you see Rich Pethia's and Dave McCurdy's valid signatures on John Doe's key, you can have a high level of trust in John by inference.

On the other hand, if you receive a key signed by a hypothetical group named, say, Computer Criminals Consortium, you have a much lower level of trust in the owner of the key that group signed, even after you've validated the key. Of course, you should never trust an invalid key from anyone.

In the case of the CERT/CC, the key certificate contains the signature of the Networked Systems Survivability (NSS) Program, the program at the Software Engineering Institute that is the home of the CERT/CC, the CERT Analysis Center, and projects related to computer security.

You can check the signatures you find in the key certificate the same way you check a PGP signature in a document.

Using PGP to Check Signatures

Although specific "how to" steps vary according to the particular PGP software program you use, you can follow these general steps to check digital signatures.

1. Get the PGP program, which is currently available both as freeware and commercially. Visit http://www.pgp.com or, alternatively, look into GnuPG for UNIX at http://www.gnupg.org.
2. Install the PGP software or have someone install it for you.
3. Check that you have a public key ring. The name of the default public key ring is often called *pubring.pkr*, though this may vary depending on the particular software program you get.
4. Add the CERT/CC key to your key ring. You can download it from https://www.cert.org/pgp/cert_pgp_key.asc. It's a good idea to refer to our web

page on encrypting sensitive information to get more information about our key: https://www.cert.org/contact_cert/encryptmail.html

5. Get the "fingerprint" of the key according to the instructions for your particular version of the software.

6. Verify the fingerprint by calling the CERT hotline 1-412-268-7090 during regular business hours—8:00-5:00 EST (GMT –5)/EDT (GMT –4) Monday through Friday. You can also check our encryption web page, mentioned in step 4. Or use this paper—the fingerprint is

   8F E3 1F 95 94 BE FD E7 9B EE 92 06 D7 35 AC F5.

   The important thing is to use an "out-of-band" method for verification. Verification can be undermined if you use the same method for all communication about the key.

7. When you receive a PGP-signed document from the CERT/CC, you can check the signature. The method varies according to your software, so you might need to consult someone in your organization for exact instructions.

You can add keys of others who give you PGP signed or encrypted files. An important thing to remember as you decide to add public keys to your key ring is that *they might not belong to the person indicated by the key certificate.* Out-of-band verification and trusted, verified signatures are important.

Appendix: References and additional information

Web pages

The comp.security.pgp FAQ

http://www.uk.pgp.net/pgpnet/pgp-faq

List of links to various FAQs (Frequently AskedQuestions) on PGP [quality varies]

http://www.landfield.com/faqs/pgp-faq/

The CERT/CC PGP key and fingerprint

https://www.cert.org/contact_cert/encryptmail.html

“Email: A Postcard Written in Pencil” [an informal explanation of why digital signatures and encryption are important]

http://www.cert.org/homeusers/email_postcard.html

Books

Garfinkel, Simson, *PGP: Pretty Good Privacy.* Sebastopol, CA: O’Reilly & Associates, Inc., 1995.

Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* 2nd ed. New York, NY: John Wiley and Sons, 1996.

Stallings, William. Protect Your Privacy: The PGP User's Guide. Englewood Cliffs, N.J.: Prentice Hall PTR, 1995.