Enabling a New PGP Key: 
Maintaining the Web of Trust (1)

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

This is the first of three brief articles about PGP and how to enable someone's new PGP key.

I received an e-mail message from an old friend today (as I write this text); he said that he had lost his PGP keyrings and had to generate a new keypair, so here was his new public key.

You will recall that Pretty Good Privacy (see <http://www.pgp.com/products/dtop-security-data/default.asp> for more information about the commercial version and <http://www.pgp.com/products/freeware/default.asp> for the free non-commercial version) generates two keys at a time (a key pair) that are complementary: what one key encrypts, the other decrypts and vice versa. One of the keys is made public; the other is kept secret by its user. This asymmetric encryption algorithm makes possible the public-key cryptosystem and that is very useful indeed.

Suppose you want to send a message securely using PGP (or any other public-key cryptosystem) so that only the desired recipient can read it: what do you do? Answer: you encrypt the message with the recipient's public key; then only the recipient knows the secret key with which to decrypt that message. (Actually it's a bit more complicated than that – the message gets encrypted with a temporary key – a session key – and then that key gets encrypted using the recipient's public key and sent along with the encrypted message.) The encryption process also ensures that the recipient can verify the integrity of the message: any change to the ciphertext – as the encrypted text is known – is detected during the decryption phase.

Now suppose you want to send a non-confidential message to one or more recipients; you want to maintain proof of integrity and you want your correspondents to be sure the message actually came from you. PGP generates a function of your message called a hash; it then encrypts the hash using your own private (secret) key. After delivery, the recipient's PGP program generates the hash of your message again; it also decrypts the hash you sent along with your message using your public key. If your decrypted hash matches the recipient's hash, then (a) nobody changed the message in transit; and (b) the message must have come from a person with access to your secret key. To the extent that the recipients are confident in your ability to protect your secret key against unauthorized use, they can have the same confidence that the message actually came from you.

In the next column of these two, we'll look at how to verify the legitimacy of a new PGP key.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.
AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at <http://www.atomictangerine.com>.

Copyright © 2000 M. E. Kabay. All rights reserved.

Permission is hereby granted to NetworkWorld Fusion to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.