Enabling a New PGP Key:
Maintaining the Web of Trust (3)

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

In the third of three articles about trusting PGP keys, we look at how to handle receiving a new PGP key from someone — and ensuring that it really does come from the person identified in the key. In the last article, I showed how easy it is to contact the sender and compare PGP fingerprints to be sure that the key did not come from an imposter.

Going one step further, I signed Bob's key using my own PGP secret key. Anyone trusting me would know that I had established to my own standards of rigor that the key was legitimate. If these third parties decided to trust my judgement, they could then use Bob's signed public key without having to check it further. Thus my verifying that fingerprint was an essential element in the non-hierarchical web of trust that underlies PGP and similar public-key cryptosystems.

Should someone who had no idea who I am trust my signature on Bob's public key? Not necessarily. They could look at who signed my public key (the public key should be stored on a public keyserver for access by anyone) and if they saw a valid signature from someone whom they did trust, then maybe they could hope that I would maintain the same level of trust. However, none of this provides formal guarantees of trustworthiness. It's an informal web of trust and it works only as well as the honesty and care of the people involved. At a fundamental level, exactly the same issues of probity and trustworthiness underlie other mechanisms for defining the level of trust in any public key infrastructure.

Anyone critically concerned with the validity of a public key can check its fingerprint by contacting the owner of that key before accepting its authenticity.

Finally, I gave my friend some good-natured ribbing: there is no reason he should have lost his PGP keyrings at all. They should be backed up safely.

In summary, there are several major lessons here for anyone using PGP:

(1) If you receive a new public key from someone you know, communicate with the ostensible owner using a trustworthy channel and check the key fingerprints before trusting the new key.

(2) When deciding whether to trust a public PGP key, you can examine who has signed the key and check the validity of those signatures.

(3) You may go so far as to check a proposed public key by verifying that key's fingerprint with its owner using a trustworthy channel of communication.

(4) If you know the owner of a new PGP key personally and you have verified the key to the maximum level of confidence that you deem appropriate, you may sign the new key if you feel that others know you and trust your judgement in guaranteeing the new key's authenticity.
(5) Back up your PGP keyrings.

***

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 Network World 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.