PGP Key Signing Party at UCITPS

From:	Stephen Lau <stephen.lau@UCSF.EDU>
Reply-To:	stephen.lau@ucsf.edu
To:	UCITPS-L@LISTSERV.UCOP.EDU
Subject:	PGP/GPG Key Signing Party at UCITPS
Date:	Tue, 24 Jul 2007 16:10:12 -0700

As part of the UCSIRC charter, every member of UCSIRC is required
to use PGP for incident information sharing. In order for this to
work, a "web of trust" needs to be developed for the keys.

To start this "web of trust", you're all invited to a key signing
party to be held at next week's UCITPS meeting. Unfortunately,
refreshments will not be served and entertainment will be
limited to whatever sheer pleasure you derive from
having your public key vetted by your colleagues.

For this party to work, YOU need to do the following BEFORE
coming to the party:

1) Generate a PGP/GPG key
2) Upload your PUBLIC (not your private) key to a public
   key server.
3) Print multiple (at least 20) copies of your public
   key fingerprint on small slips of paper with your name
   on them.
4) Bring the slips of paper with you, along with a valid UC
   ID to the key signing party.

Ugh, you may be saying, what does all this mean? Well, here's some
additional information...

For a general overview, look here:
http://www.cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.html

For PGP: http://www.pgp.com/index.html
PGP is the commercial version and comes with a nice GUI.

For GPG: http://www.gnupg.org
GPG is a GNU version of PGP and interoperates nicely.

Uploading Your Key
==========
There are numerous public key servers. Both PGP and GPG allow you
to upload your public key. You can also manually export your public
key and upload them to a public key server.

Here is a decent public key server to use:
http://pgp.mit.edu/

You can use the pgp.mit.edu to look up my public key as an example.
Simply type in "Stephen.lau@ucsf.edu" in the search field. Select
verbose index and you will see that my key has been signed by
multiple people.

Printing Your Fingerprint
==========
Key fingerprints are not the public keys. It's a block of 10
4 digit hexadecimal numbers. For example, my PGP fingerprint
is: "44C8 C9CB C15E 2AE1 7B0A 544E 9A04 AB2B F63F 748B" and can
always be found in my email signatures. They are used to
verify that the public key you have is the one you want.

Refer to your PGP client to determine how to extract the fingerprint
from your PGP key. Print the fingerprint along with your name
onto small strips of paper. These strips will be distributed to
other attendees so they can go and download your public key and verify
them by the fingerprints printed on the slips of paper.

Colleagues Who Can Not Attend
==========

By the general guidelines for PGP web of trust building, one must
have face to face presence to vet each other's keys. If you
have colleagues who are not able to make it, you will not be allowed
to share their public keys in this venue. Since *you* know your
colleague, *you* can sign their keys and it will be up to individuals
if they wish to have transitive trust.

Feel free to ask any questions.

Steve

--
+---
Stephen Lau - Stephen.Lau@ucsf.edu
Information Security Policy and Program Manager
University of California, San Francisco
1855 Folsom, Suite 602, Box 0707, San Francisco, CA 94143
+1(415) 476-3106 (Work) +1(415) 476-1717 (Fax)
PGP: 44C8 C9CB C15E 2AE1 7B0A 544E 9A04 AB2B F63F 748B
+---