Pretty Good Privacy (PGP)

Introduction to Key Management

(Based on Materials originally from Joe Abley, AfNOG 2006)
April 18, 2007

Introduction

Check the GnuPG web page for documentation on the GnuPG package:

http://www.gnupg.org/

In particular, look at the documentation, and the "Mini HOWTO" which is good background material for the topics in this workshop.

Do you want to use the key generated today?

If you wish you can save the public/private key pair that you generate today and use them when you go home. This can be very useful. To do this, then you will want to copy the contents of the directory ".gnupg" on to something like a memory stick before you finish this workshop. Remember to protect these files from others. As this workshop is fairly open and people can gain access to your machine you certainly must use a good passphrase, when asked, to protect your private key.

Public Key Cryptography

Key Concepts Review

1. Public key cryptography uses two related keys -- a secret (or "private") key, which is never shared and which should always be kept in a secure place, and a public key. The public key can be shared with anybody.
2. To encrypt some data so it can only be read by one person, you need that person's public key.
3. To decrypt some data that someone sent you, you need your secret key.
4. To sign some data, you use your secret key.
5. To check a signature on some data, you use the public key of the person who used it.

Two Precautions Worth Taking

1. Before you use someone's public key, make sure you trust it. That is, be sure that the public key was not modified in between the owner and you. You can increase your trust by comparing the fingerprint of the key you have with that calculated by the key's owner. You can also gain some measure of trust by checking signatures that might be present on the key.
2. When you are talking to the owner of a public key, either directly in person or via telephone, think about how much trust you have in the identity of that person. Use measures like the reputation of the person amongst other people you trust, matching photo i.d. (e.g. passports) and the person's knowledge of shared experiences in the past to gain a level of trust you are comfortable with.

Install GnuPG

On FreeBSD, GnuPG is included in the ports tree as security/gnupg. To check and see if GnuPG is already installed first do:

```
# pkg_info | grep gnupg
```

If you don't see something like this:

```
“gnupg-1.4.5_1        The GNU Privacy Guard”
```

Then it is not installed. To install GnuPG do the following as root:

```
# portinstall gnupg
```

Creating a Public/Private Key Pair

Now that GnuPG is installed you can use the `gpg` command to use the Gnu version of PGP. In these steps you should do this as your user on your system, *not* as the root user! *Remember, do this with your username, not the root account*:

```
$ gpg --gen-key
```

You will quite a bit of output on your screen. When presented with:

```
Please select what kind of key you want:

   (1) DSA and Elgamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)

Your selection?
```

Simply <PRESS ENTER> for the default selection of DSA and Elgamal. Now you will be asked for what keysize you would like to use.

```
What keysize do you want? (2048)
```

Again, <PRESS ENTER> to accept the default of 2048.

```
Please specify how long the key should be valid.
         0 = key does not expire
<n>  = key expires in n days
<n>w = key expires in n weeks
<n>m = key expires in n months
<n>y = key expires in n years
Key is valid for? (0)
```

At this point enter ==> **`1y`**

To specify that your key will expire in 1 year.

You will now be asked to verify the expiration time, give your real name, email address and an optional comment. Here is a sample of this with responses. Please use your real name and email address. You do not need to enter a comment:

```
Key is valid for? (0) 1y
Key expires at Wed Apr 23 21:59:48 2008 WAT
Is this correct? (y/N) y

Real name: Mary Q. Public
Email address: mpq@stupendous.net
Comment:
```

Finally, you'll be asked if everything is OK. If you like your choices, then press “O” for “Okay” and your new PGP public/private key set will be generated.

```
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

Now you are asked for a passphrase. You can type in something long (very long) or short. But, you want something fairly complex to be secure.

```
You need a Passphrase to protect your secret key.
```

After you enter in your passphrase (twice), then you'll see a a bunch of stuff on your screen as your keys are generated.

The GPG software will create a Public/Private key pair using random information it obtains from the system. If it seems to be taking a long time, try to keep the machine busy by using the network or the keyboard, since both those things are used to add randomness to the key generation process.

Your PGP information will be stored in your user's account home directory under the directory called “.gnupg”.

Extracting your Public Key

To extract your public key as text which you can easily cut and paste, or include in an e-mail message, do:

```
$ gpg -a --export <your key id>
```

Note: "your key id" is probably your email address.

The key id is a hexadecimal number that will have been displayed after you generated your key. If you know you only have one key which matches your e-mail address, you can use your e-mail address instead of the key id, and everything should work.

To see what public keys you have installed, you can always type

```
$ gpg --list-keys
```

Public keys are installed by receiving a user's public key as a text file (say in email), saving it, and importing it in to your local PGP public key ring. Or, perhaps, you have a PGP plugin installed for your local email client. You may import public keys this way as well.

Once you have extracted your public key, you can send it to other people. Good ways of doing this are e-mail, putting it on a web page, or sending it to a key server.

For instance, to place your newly generated public key on the MIT (Massachussetts Institute of Technology in Boston, Massachussetts, United States) PGP server you can do the following:

- Go to http://pgp.mit.edu/
- Choose "Submit a Public Key"
- Copy your Public Key text in to the text box on the page
- Press "Submit"

That's it! Your public key is now available to anyone who goes to the MIT PGP server and searches on your name, email address, etc. This is a good thing.

Generating your Public Key's Fingerprint

Comparing public keys is difficult, because the keys themselves are usually quite long. A much easier method (and, in practical terms, pretty much as good) is for each person to generate the fingerprint of their copy of a key, and then compare the fingerprints. Fingerprints are short enough to be easily read out over the phone.

You calculate the fingerprint for a local copy of a public key like this:

```
$ gpg --fingerprint <key id>
```

Importing Someone Else's Public Key

Once you have obtained a public key, you can import it to your local keyring so that you can use it like this:

```
$ gpg --import <filename>
```

Signing a Public Key

If you have a copy of someone else's public key on your keyring and you have decided that you trust it (e.g. by verifying the fingerprint with the key's owner) and you have also decided that you trust the identity of the key's owner (e.g. by checking a passport) you can sign it. This does two things:

1. It helps you remember in the future that you have checked the key, and it is to be trusted.
2. If other people receive a copy of the key with your signature, and they trust you, then they can use your signature to help them decide whether they trust the key. This helps build what is known as "the web of trust".

To sign a key:

```
$ gpg --sign-key <key id>
```

Key Signing Party

At some events you may see announcements for a PGP Key Signing party. This is when a group of people get together, bring some form of ID (passport, drivers license, etc.), verify each other's identies and agree to sign one and another's public PGP keys.

If your instructor remembered to ask you to bring your passports, etc. to this session, and if there's time we'll have a key signing party right now. If not, then perhaps one can be arranged later.

More Information

There are many more things you can do with GnuPG than those described in these notes. For more information, see:

> http://www.gnupg.org/

Of course, you can also ask your AfNOG friends on the AfNOG mailing list, or send e-mail to the instructors directly if the GnuPG documents are not clear.