System Administration for Beginners

Week 11 Homework

May 4, 2009

Please turn in your homework by the beginning of class, with the assignment title, your name, `inst` login, and the answers (if multiple choice, just the letter is fine).

1 Introduction

In lecture, we've explored Cryptography and Encryption focusing on the Gnu Privacy Guard implementation, **GPG**. Now you will learn this directly by using **GPG** to share files and send emails.

2 Homework

You will be working with your partners for this homework. First of all, you will need to create your own PGP keypair. This will only be used for the homework. Do not expect this to be used outside of the decal. We are not considering the full implications of a PGP key in this homework because we would need to dive into the security, privacy, and identity implications which is beyond the scope of this course.

Create your keypair. Use your full name for name and your login@ocf.berkeley.edu for the email. As a comment, type in your inst account name.

1. What types of keys can you make and what are the limitations for each?
2. You have to specify a keysize. Why is this important?
3. After you specify the options, the program will actually create the key based on entropy. Why does it need entropy and where does it come from?

Now that you have a keypair, share your public key with your partners. We will share the keys via files rather than through a public keyserver since these are not intended for public use.

1. Export your key to a file: `gpg --export --armor KEYID > public.key`
2. Place a copy in your webspace: `cp public.key  /public_html`

3. Import your partner's key: `gpg --import public.key`

4. Verify the key fingerprint: `gpg --fingerprint KEYID`

Now you can share files with each other signed and/or encrypted

1. Create a file and sign it with your key. Send it to your partner and have him/her verify the signature.

2. Create a file and encrypt it to your partner's public key. Send it to your partner and have him/her decrypt the file.

In addition to sharing files, you can also send emails. Here is a short tutorial on how to use the program **mutt**: `http://www.ucolick.org/~lharden/muttchart.html`, and a short section of the manual relating to gpg: `http://www.mutt.org/doc/manual/manual-2.html` (Using Mutt with PGP).

1. Send an email to your partner that is signed and verify the signature.

2. Send an encrypted email to your partner.

3. Send a signed email to jchu+decal@ocf and cardi+decal@ocf that contains the location to your public key accessible via email. Subject: [HW10] LOGIN Signed Email

4. Send an encrypted email to us with your name, your major, and something random. Subject: [HW10] LOGIN Encrypted email

3 Turning in Homework

We expect you to turn in homework at the next class answer each of the questions above and the commands you used for each. Furthermore, we expect two emails from you.