CSCI 530 Lab 2

Public Key Infrastructure
Date assigned: 1/26/2006 3:30 PM
Date due: 2/5/2006 11:59:59 PM

Overview

In this lab, students will set up a personal e-mail client, thunderbird. Students will install the thunderbird plugin, Enigmail. Students will create a DSA digital signature and practice sending and receiving digitally signed e-mail.

Instructions

1. Setting up Thunderbird
    a. Download Thunderbird from http://www.mozilla.com/
    b. Install Thunderbird, following the instructions shown.
    c. Configure Thunderbird, following the instructions on the Information Technology Services webpage at USC: http://www.usc.edu/its/email/readers/thunderbird/
    d. Download the GnuPG Binary Package, at http://www.gnupg.org/download/index.html
        i. The direct link for the windows download is ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.6.exe
        ii. If you've already had GnuPG installed on a system, you may want to research more as to saving and loading your keyring, as these instructions assume that you've never installed any PGP tools on the system
    e. Download the Enigmail extension at http://enigmail.mozdev.org/
        i. In your browser, right click on the link after you've selected the download link. Otherwise, Enigmail might try to install itself (if you use Firefox).
    f. Open up Thunderbird, and go to Tools → Extensions
    g. Click on Install
    h. Select the Enigmail extension you downloaded above.
    i. Restart Thunderbird. Enigmail will now load.
    j. When you reload thunderbird, the OpenPGP wizard will open. "Select No, that you want to configure things manually" and hit next.
2. Generate a new keypair
    a. Go to OpenPGP → Key Management
    b. Go to Generate → New Key Pair
    c. Enter in a passphrase for you to remember
    d. Click on Generate
    e. Create the revocation key (hit yes, and then enter your passphrase)
3. Add this key to the keyserver at pgp.mit.edu
    a. With the Key Management window open, right click on your key
    b. Select "Upload Public Keys to Keyserver"
    c. Enter "pgp.mit.edu" as the keyserver

d. Open up your web browser, and go to the URL pgp.mit.edu
e. Go to Search String, and enter your name to confirm that your public key has been uploaded.

4. Sign my key
    a. With the Key Management window open in Thunderbird, go to Keyserver → Search for Keys
    b. In the Search for key, enter "Joseph Greenfield", and for the keyserver, enter pgp.mit.edu
    c. Look for the key with the Key ID 729C21D9. This is the only key you need. Click on the box next to that key, and hit okay. You will see that the key has been added to your keyring, but it is not in bold. This means you are not the owner of this key.
    d. Right-click on that key, and select "Sign Key"
    e. You will have 4 levels of trust for signing my key. You may choose any of the above. I would recommend "I have done very careful checking" or "I have done casual checking."
    f. Right-click on that key, and select "Set Key Trust"
    g. You will have 5 levels of key trust. You may again select how much you trust me.
    h. Click CTRL-A to select all the keys, and go to Keyserver → Upload Public Keys. You have now digitally signed my key and uploaded it back to the Keyserver.
5. Send an e-mail with a digital signature
    a. Open up Thunderbird
    b. Click on the button that says "Write"
    c. Compose an e-mail to my e-mail address joseph.greenfield@usc.edu
        i. In the subject line, put "Digital Signature"
        ii. In the body, put your name, e-mail address, student ID, and what lab section you are in. If you are a DEN student, state that you are a DEN student in the e-mail.
    d. Click on the OpenPGP Button
    e. Check the box that says "Sign Message". Hit okay.
    f. You will see a little green pencil in the bottom right hand corner of the e-mail. This says that the e-mail will be digitally signed.
    g. Hit the send button
    h. You have now sent me an e-mail that has been digitally signed by you.

Assignment

Send me a digitally signed e-mail exactly as above.
Answer these questions and upload them to blackboard.usc.edu. Go to assignments, and under labs, click on Lab 2 for submission.

1. Are there other ways of authenticating e-mail? What are the benefits of these other methods compared to PGP. What are the downsides?
2. Enigmail allows you to either digitally sign your e-mail, encrypt it, or both. Give scenarios where you would only want to digitally sign the e-mail, only want to encrypt it, and where you would want to do both.
3. Are there other applications for PGP aside from e-mail? Give examples.