Homework 8

HOMEWORK 8

In this assignment, you will install a PGP encryption tool on a computer, and exchange PGP e-mail with each other and then Mike Berger.

BACKGROUND:

PGP is a standard format for encryption and digital signatures. It is supported by a number of different software programs. You may use any tool that accurately implements the PGP standard, and we make some recommendations below.

For background, read the first half this overview of PGP here (up to but not including "digital certificates"): http://www.pgpi.org/doc/pgpintro/

(We will not be using PGP certificates in this assignment)

I wrote a paper in 1999 on how difficult it was to use commercial PGP software during that time period. Please read it: http://www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/USENIX.pdf

If you do not already have PGP installed on your computer, there is an important decision for you to make: whether you will upload your public key to the public keyservers (such as https://pgp.mit.edu/). Uploading will allow others to easily find your public key and then send you encrypted e-mail. However that listing is public, so it will expose your name and e-mail address (and may cause you to receive some spam.) We do not require you to upload your key with public key servers, but you are welcome to do so. (The tutorial for GPGTools below assumes you want to list your key with public key servers. If you do NOT want to list your key with public key servers, do not check the box "Upload public key after generation.") You can always upload your key at a later date, but once you upload it, you will not be able to delete the entry.

Finally, when we refer to signing and encrypting an e-mail message, you should always sign first and then encrypt. When we refer to decrypting and verifying an e-mail message, you should always decrypt first and then verify.

CHOOSING A PGP PROGRAM:

You may use any PGP tool you wish that accurately implements the PGP standard. In this section, we give some recommendations.

For MacOS, a popular tool is GPGTools: https://gpgtools.org/ Here is a tutorial on GPGTools: http://notes.jerzygangi.com/the-best-pgp-tutorial-for-mac-os-x-ever/

You should be aware that in the future (after the release of Yosemite) GPGTools will no longer be free, but currently it is still currently free.

For Windows and Linux, a popular (Java based) tool is PortablePGP: http://ppgp.sourceforge.net/
Here is a tutorial on PortablePGP (skip the first half which discusses another tool, PGP Desktop): http://www.pgpguide.20m.com/

After you install PortablePGP, you need to change the permissions on the public.bgp file. On the instructor's machine, this is located in the folder C:\Program Files (x86)\PortablePGP . Go to that folder, and right click on `public.bgp`. Choose "Properties", then choose "Security". Click on "Users" and then on "Edit". Make sure that "Full control" - "Allow" is checked.

(The MacOS tutorial listed above is much more detailed than the Windows tutorial, so you may enjoy reading it even though it is not applicable to Windows installations.)

If you use Outlook as a mail client, you may want to use GPG4win instead: http://www.gpg4win.org/ Here is a tuorial on GPG4win with Outlook: http://www.triatechnology.com/sending-a-pgp-encrypted-email-in-outlook-or-webmail/

PREPARATION

Find a partner -- you will be doing this assignment in pairs (or groups of three). Unlike other assignments which did not allow collaboration, you are fully able to collaborate in this assignment. Each member of a team should generate a PGP key pair (or alternatively import your existing key pair into your PGP tool.)

Export your public key and share with your team member(s) (don't give away your secret key). Add the public keys to your keychain or keyring.

With your team members practice signing and encrypting and then sending secure e-mail. Also practice decrypting and verifying secure e-mail. Make sure you are completely comfortable with this.

PHASE 1 (due at 11:59PM, Thursday, October 23, 2014)

Look up mjberger@gmail.com's public key. If you are using GPGTools, you can do this by typing Command-F. Otherwise, you can find it from the MIT Public Key Server (https://pgp.mit.edu/). Save the public key in a text file.

If you are running PortablePGP, click on Key ring. Click on "Public Keys" and the down arrow. Choose the text file that you save Mike Berger's public key in. That should install Mike Berger's public key in your key ring, and you will now be able to encrypt in his key and verify his signature.

The team send two e-mail messages to Mike (only one account needs to do this). Make sure both e-mails list all the members of your team. The first e-mail will not be encrypted, and but will contain your exported public key. The second e-mail should contain at least a 50 word message and should be signed by you and encrypted in Mike's public key.

PHASE 2 (due at 9AM, November 4, 2014)

Mike will send the group back an e-mail. Decrypt the e-mail, and verify Mike's signature. (If the signature is not valid, send him a signed and encrypted e-mail asking him to send an e-mail with a correct signature.)

Once you get a message with a valid signature, read it: it will contain a list of questions to answer in a write-up. Each member of the team should answer the questions on his or her own.

Put your write-up in hw8.<lastname>.txt or hw8.<lastname>.pdf and use the file upload tool available at https://www.ischool.berkeley.edu/uploader/?s=i206 (login with your ISchool userid and password).

hw8