ITP 125 - Lab 07

Deadline

1 minute before the next scheduled lecture.

Objective

Learn to use asymmetric encryption.

Questions

1. Look over what we did in this lab. How do we securely email multiple people at the same time? Hint: Play around with Thunderbird.

**You can add multiple keys and will generate the corresponding hash**

1. Read over the following article, and do not worry about understand everything that is said:

<http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance>

Bruce Schneier is a pretty famous security researcher. After reading the article do you feel you can stay secure from NSA spying on you?

**There are pretty much holes everywhere in cybersecurity, I’m sure the NSA has access to exclusive backdoors that we are not aware of**

1. In the article it mentions air gap:

<http://en.wikipedia.org/wiki/Air_gap_(networking>)

If you have sensitive information do you think this protection is enough to really protect your sensitive information.

**Well the more we strip away from a computer, the more secure it is. If we have a hard drive that is just sitting in a shelf alone, that’s as secure as it gets. Air gapping is just trying to achieve that same effect. Unless we physically remove the hardware that allows network connections, there are still risks even if we do air gapping.**

1. What was your reaction the to NSA revelations? When you first heard of it, were you concerned about your privacy?

**It was a bit disconcerting to know that NSA has so much power and access. However comparing myself to the common person, the amount of “illegal” things I do is just about the same amount, so unless NSA wants to arrest millions of people, I think I’m just fine.**

1. Read over the following site:

<http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>

Did you perception of NSA activities change? Did you learn anything from the site?

**Didn’t read it, have to study for midterm.**

Submission

In addition to uploading your key to **keyserver.pgp.com**, you will upload your **public key**, to the USC web hosting. Rename your public key as, **public\_key.asc.** The \*.asc file will be your submission.

Answer the questions above. **Encrypt the file using the instructor's public key**, and name it **lab07.docx**. Upload the file to your **itp125 folder** on the web hosting.

Make sure you can see the file by publicly accessing the URL using any web browser of your choosing.

FAQ

1. **Question:** I have no idea what I'm doing.

**Answer:** Before you leave the class make sure you take with the TA, Instructor, or fellow students for help. Do not leave the room before you understand what is going on. You can always use the power of Google/Yahoo/Bing to figure it out.

1. **Question:** How do I encrypt the file?

**Answer:** Check out the section call “Encrypt and Decrypt Messages with GPG” on the following link:

<https://www.digitalocean.com/community/tutorials/how-to-use-gpg-to-encrypt-and-sign-messages-on-an-ubuntu-12-04-vps>

1. **Question: Will I need to use encrypted emails to communication with the instructor?**

**Answer:** Why would you be doing this if that is not the case? If you send and unencrypted email it will go straight to trash. Now there will be exceptions to this rule.

1. **Question:** When I check out the itp125 using a web browser, I get a page that says “Forbidden”

**Answer:** This is a permission issue with the files that you have uploaded. You can fix this issue by logging into aludra.usc.edu using ssh. Then run the following command:

**chmod –R a+rx public\_html**

What the command will do is change the permissions on the folder **public\_html** so that everyone (**a**) can read and execute the files (**+rx**). In addition, it will change the permissions for everything within the **public\_html** folder, including folders within it (**-R**)

1. **Question: Cannot find your public key...**

**Answer:** <http://www-bcf.usc.edu/~chiso/itp325/public_key.asc>

1. **Question: Is it possible to do with without installing GPG Tools for OSX?**

**Answer:** No. You won’t be able to encrypt the file from Terminal with Mailvelope alone. If you happen to find another way to encrypt the files with my public key, you can do that instead.

Videos

Remember these videos are just examples. You will need to adjust the command to match your needs for the assignment.

**Windows GPG File Encryption**

The commands involving GPG can be used on OSX as well.

<https://youtu.be/sPmW8Y2LMaM>