

# ECE646 – Fall 2007

## Lab 2: Pretty Good Privacy - ChEaTiNg

### PLEASE READ THE FOLLOWING INSTRUCTIONS CAREFULLY:

1. A LAB REPORT must be handed in at the beginning of class on **Wednesday, October 10th**.
2. You are required to address all the questions listed in this manual in your final report.
3. All e-mails exchanged with other students as a part of this lab should be CC: to [gmuece646@gmail.com](mailto:gmuece646@gmail.com)

In LAB 1 of PGP, you have seen the how PGP works by studying its Encryption, Decryption, Key Exchange, Direct Trust mechanisms.

In this LAB, you would be exploring the security of PGP against cheating. You will be creating Fake KEYS to impersonate some of your classmates and study the vulnerabilities caused. Please make sure, you CC all communication to [gmuece646@gmail.com](mailto:gmuece646@gmail.com) and also ensure that your using the right subject line (mentioned in each section).

In order to perform the following lab, you are required to have an understanding of **LECTURES 1-4** and have read the following sections:

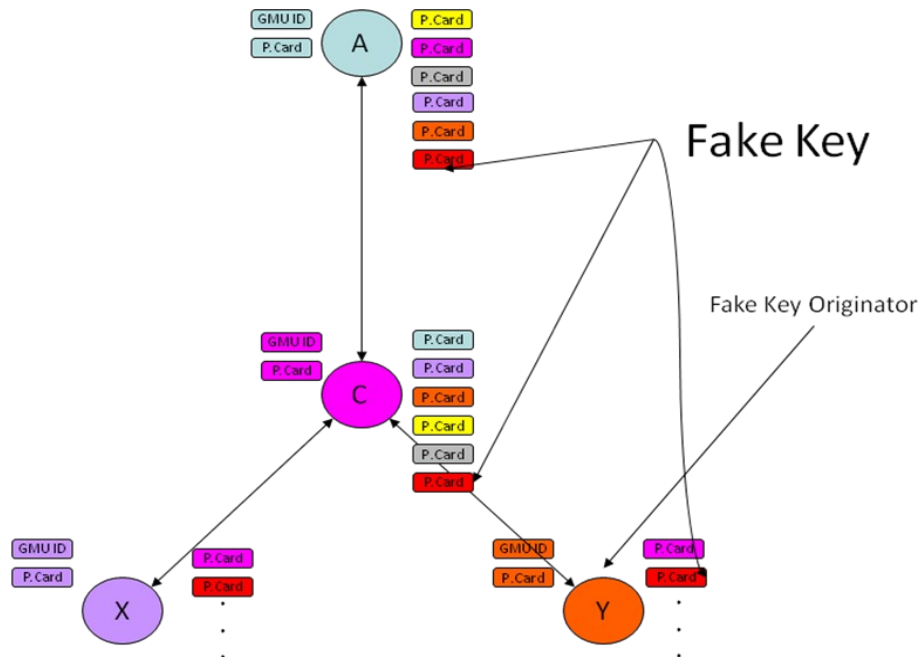
- Stallings, 4th ed., Chapter 15.1 and appendices 15 A, B, C, or
- Stallings, 3rd ed., Chapter 15.1 and appendices 15 A, B, C, or
- Stallings, 2nd ed., Chapter 12.1 and appendices 12 A, B, C.

## 1 STUDENT LIST

The full list of students registered for the course will be provided via an e-mail to your gmu address.

Create a new email accounts for a **MAXIMUM of 2 students**, who are not already a part of your Direct Trust Group. Associate these email IDs with newly created public/private key pairs. You may register these keys in the GPG Global Directory.

## 2 WEB OF TRUST



Create and sign 3 different versions of your public key ring.

- One version should be entirely correct ( 3 genuine keys)
- 1 Fake public key/account name pair + 2 genuine keys
- 2 fake public key/account name pair + 1 genuine key

Send these public key rings to the members of your **DIRECT TRUST GROUP**. Assign the public key rings to these people by your personal preference, following the general rule that you would rather cheat on strangers than on your friends. Please remember to CC: your communication to [gmuece646@gmail.com](mailto:gmuece646@gmail.com), with subject line as "**LAB2 KEYRING:**"

Once you receive a Public key ring from your any of the member of your DIRECT TRUST GROUP, import them to your PUBLIC KEY RING.

### Questions:

1. List all the fake email IDs created with there public/private key pair.
2. Draw the Hierarchical Diagram showing your public key ring web of trust.

### 3 MESSAGE EXCHANGE BY EMAIL

At this point you should have in your public key ring public keys of at least 9 people you did not exchange public key cards. **CHOOSE CAREFULLY 3 OF THEM**, to whom you will send messages. Base your decision on the trust assigned to their introducers and the key legitimacy fields associated with their public keys, and filled automatically by PGP.

- Send encrypted and signed messages to three classmates selected in the previous step. As a part of each message ask a simple question of your choosing.
- **RESPOND TO ALL EMAILS** you have received using your own email accounts, and using any faked email accounts you have created. Encrypt and sign your answer.
- Keep record of all messages and include them as an appendix to your report. Please remember to CC: all your communications to [gmuece646@gmail.com](mailto:gmuece646@gmail.com).

**YOU WILL RECEIVE '1 EXTRA POINT' FOR EACH EMAIL RECEIVED AT THE FAKED EMAIL ADDRESS, AND '-1 POINT' FOR EACH EMAIL SENT TO A FAKED EMAIL ADDRESS.**

**Responses to fake addresses do NOT carry a penalty!**

#### Questions:

3. **Was any of your attempts to cheat successful? If no, why? If yes, what was the major weakness of the key distribution procedure used in this exercise that has made your attack successful?**
4. **Where you able to identify, if a public/key ring received was fake? If yes, How? If no, why?**

### 4 PGP Global directory

- Search the Global Directory by name for keys belonging to three classmates outside of your web of trust.
- Send encrypted and signed emails to these three classmates, ask a simple question of your choice.
- **RESPOND TO ALL EMAILS** you have received using your own email accounts.
- Encrypt and sign your answer.
- Keep record of all messages sent and received and include them as an appendix to your report. Please remember to CC: all your communications to [gmuece646@gmail.com](mailto:gmuece646@gmail.com).
- There are no extra points and no penalty points for this part of this lab.

#### Questions:

5. **Was any of your attempts to cheat successful? If No, why? If yes, what was the major weakness of the PGP Public Key Directory that has made your attack successful?**