Mittuniversitetet
MID SWEDEN UNIVERSITY

DT116G Network Security

Laboratory Assignment: Privacy of Communication

Daniel Bosk
daniel.bosk@miun.se

Lennart Franked
lennart.franked@miun.se

lab_PoC.tex 1242 2013-09-02 11:11:14Z danbos

Contents

1 Introduction

This laboratory assignment will cover how public and private keys are used in practice, how to use these to encrypt and decrypt as well as sign and verify a message or a file, also some basic key distribution. We will also cover alternative ways to try to evade prying eyes from finding your message. We will use the open source programs GNU Privacy Guard (GPG) and OpenPuff.

2 Aim

After completion of this assignment you will

- Have an understanding of how to use a public–private key-pair.
- Know how to use implementations of asymmetric ciphers.

- Be able to distribute your own key and retrieve other public keys using publicly available key servers.
- Be able to use steganography as a way to hide messages.

3 Reading instructions

Before starting this assignment you should have read chapters 1–4 and 8 in *Network security essentials : applications and standards* [3].

For the second part of this assignment you should read *OpenPuff v4.00 Steganography & and Watermarking* [2] to fully understand how steganography works in practice.

During this assignment you should consult the documentation for instructions on how to use the specific softwares [1, 2, 4].

4 Tasks

This assignment is divided into two parts. The first part will cover email security, and the second part will cover steganography.

4.1 Email security

In this part you will work with email security. You will start by creating your own key pair after which you will upload your public key to one of the public key servers. Once you have done that you will send an encrypted email to one of your classmates which will be your lab partner. You should be able to find his or her public key on the key servers. Start by downloading and installing GPG, select the appropriate version of GPG depending on what operating system you use. Once you have GPG installed on your system, generate a key pair and *make sure to make an active choice of what cipher and key size to use.* When finished, export your public key to the following key server:

`keys.gnupg.net`

Next you shall import both your partner's key and your tutor's key, they should be available on the same key server. When you and your lab partner have each other's public keys, send an encrypted email to each other and confirm that the other party is able to decrypt your email. Next find a way to communicate with your partner, such that you can confirm that they are who they say they are, and ask them to repeat the fingerprint of their public key. Once verified you can publicly sign their public key with an approprite trust level based on the type of verification you did. When you have completed these steps you must send an encrypted email to the tutor and await an encrypted response.

4.1.1 Social engineering using spoofing (optional)

Try to trick a different classmate using a spoofed email or an other form of communication, that you are their lab partner. Will you be able trick them into believing that your fingerprint is their partners? What measures must be taken in order not to be tricked?

4.2 Steganography

In this part you will work with steganography. By using the program OpenPuff you will get a practical understanding of how steganography works.

Start by installing OpenPuff, you can find the program at the following URL:

`http://embeddedsw.net/OpenPuff_Steganography_Home.html`

Once installed, write a message in a text-file and hide it in a picture. You will then post this picture in the course forum, where your partner can access your picture and retrieve the hidden message. Use GPG to exchange the secret passwords publicly in the forum without anyone else being able to read it.

4.2.1 Retrieving other groups' messages (Optional)

Try to retrieve a hidden message posted by another group. If retrieved, post the hidden message as a reply to that picture. You will then be eligable for the grade *Pass with Distinction* on this assignment.

5 Examination

The following results must be handed in:

- Give a short summary of your installation process, including what cipher you choose, and the key length. *You must motivate this, 'Because it was default' is not a valid motivation.*
- Explain how you verified that your partners public key was the correct one. Motivate why you chose the method you did, and based on this, how certain you are that this person actually is the same person that owns the public key.
- A copy of the secret message you received from your tutor by email.
- Using at least 250 words, give a detailed description of how steganography works.
- Any proof of that you solved the optional assignments.

References

[1] Werner Koch. *Using the GNU Privacy Guard*. Mar. 2012. URL: `http://www.gnupg.org/documentation/manuals/gnupg.pdf`.

[2] Eng. Cosimo Oliboni. *OpenPuff v4.00 Steganography & and Watermarking*. July 2012. URL: `http://embeddedsw.net/doc/OpenPuff_Help_EN.pdf`.

[3] William Stallings. *Network security essentials : applications and standards.* 5th ed. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.

[4] The Gpg4win Initiative. *The Gpg4win Compendium.* Aug. 2010. URL: `http://wald.intevation.org/frs/download.php/775/gpg4win-compendium-en-3.0.0-beta1.pdf`.