Lab 11.2: Encrypting messages with GNU Privacy Guard (GPG)
IN618 Security

May 13, 2015

Introduction

Earlier this week we saw how to manage file ownership and permission to protect data. Sometimes these measures don't provide enough security for especially important data. For these situations we use encryption. Public key encryption tools like GNU Privacy Guard (GPG) can be used for this.

Although the underlying principles of public key encryption are quite sophisticated, it is relatively easy to encrypt and decrypt files using tools like GPG. In this lab we will experiment with this software.

1 Procedure

1. Install the gpg4win package available at `I:\COURSES\EAD\AITEIT3\BITY2\IN618 Security\GPG-Lab`
2. Start the Kleopatra application you just installed.
3. Create a new certificate by selecting File → New Certificate. In the dialogue, identify the certificate with your first and last name and your OP email address.
4. Export your certificate by highlighting your certificate in the list (which should only contain your certificate right now) and clicking the "Export Certificates" button. Save your file in `M:\ICT Students\IN618 Security\Certificates\firstname.lastname.asc` (using your own name for the file).
5. Create a plain text file using notepad or something similar. Type a short message in the file. Save it to your desktop.
6. Encrypt the file by going to File → Sign/Encrypt Files. In the next dialogue box be sure that "encrypt" is chosen. In the next dialogue choose your key and hit the "Add" button. Then click "Encrypt" and note where the encrypted file is saved.
7. Try opening the encrypted file with Notepad and observe that it is indeed encrypted.
8. Now decrypt the encrypted file by going to File → Decrypt/Verify Files. Check your decrypted file.
9. Now choose a partner. Click the "Import Certificates" button in Kleopatra and navigate to the Certificates folder on the `M:` drive. Find your partnerâĂŹs file and import it.
10. Now encrypt your message again, but this time use your partner's certificate. Email the encrypted (.gpg) file to your partner.
11. Retrieve your own encrypted message from your email and use Kleopatra to decrypt it.

2 Reflection

Although we are able to send each other encrypted files and decrypt them, our process still has a major security weakness. What is it?