# Assignment 1: Cryptography

## Due Week 4, Worth 10%

**Question 1:** Security professionals need to ensure that they keep up to date with the latest threats and security issues. This allows them to update their risk profiles, such as identifying if their systems are vulnerable. In order to determine what the risk to an organisation is, you need to know what the problems could be.

In this assignment, your task is to identify a recently announced security vulnerability and write a profile of the threat. The profile should contain:

1. Name of the threat,
2. Systems it attacks,
3. How it performs its attack,
4. Mitigation strategies,
5. Discuss on the scope of the threat in terms of who could be exploiting this vulnerability (Cyber criminals or state nations),
6. Concluding reflection (100 words) on the adequacy of the mitigation strategies.

Your report should be maximum 2 pages and should contain relevant tables, calculations, a ranked list of threats (in terms of impact) and conclusions.

See the scoring sheet for this assignment and ensure that your report fulfils the criteria listed.

# Scoring Q1:

|  |  |  |
| --- | --- | --- |
| **Type** | **Score** | **Description** |
| **Content** | | |
| Systems it attacks | 7 | Appropriately highlight which systems it attacks and does the attack targets operating systems or applications or is it multilevel. Reports that go outside the bounds will lose marks from this category. |
| How it performs its attack | 7 | Complete strategy of the attack to exploit the vulnerability should be given. |
| Mitigation strategies | 7 | Reports should cover the mitigation strategies (technical, policy, training etc.) of the profile |
| Scope of the threat | 7 | Discuss on the scope of the threat in terms of who could be exploiting this vulnerability (Cyber criminals or state nations) |
| Concluding reflection | 7 | Reflection should be your views and should be clearly articulated |
| Subtotal: | **35** | Subtotal for content |
| **Presentation** | | |
| Spelling and Grammar | 5 | The presentation’s content is appropriately written in English, with no spelling errors and grammar issues. |
| Presentation and Style | 5 | The report is well presented, with diagrams, headings, tables and other visual aids. |
| References | 5 | The report contains appropriate references and referencing style. |
| Subtotal: | **15** | Subtotal for presentation |
| Total: | **50** |  |

**Question 2:** You are required to learn the **GPG**/**PGP** package using Linux Kali environment (learning the applications of private and public key cryptography to secure email messages and documents) to be able to answer the following questions. You should pair up with one of your class fellows to do this lab, record results and give commentary on the results.

If you do not have a class fellow, then create two user accounts and you can encrypt using one account and descript using other account. You should use screen shots from your experiments to support your responses.

1. Generate keys of 4 different sizes for the RSA encryption scheme and include these keys in the report. Provide a table showing key size and the key generation time. Describe the variation in key generation time and explain its cause.
2. Encrypt a file (text or binary) using **one** key and display a portion of the encrypted file using the “hexdump -Cv *filename*” command. Explain the commands used and include a screenshot of a portion of the encrypted data.
3. Create a file of 1 GB containing random data. Encrypt and decrypt it using **one** key and note the time taken. Comment on the reason why this much time is taken. Show the command used to create the file of random data.
4. Export your public key and discuss the reason why your exported key is in an ASCII format.
5. Encrypt a file containing ASCII text and display the cyphertext using the “hexdump -Cv *filename*” command.
6. You should work with your class fellow/or create two accounts to do this experiment and record your observation in the form of commands used and include screenshots of the results that were obtained.
   1. Exchange your public key and your friend’s public key using email.
   2. Import your friend’s public key into your key ring.
   3. Encrypt a file using your friend’s public key and send the encrypted file to your friend.
   4. Ask your friend to decrypt the encrypted file.
   5. You can ask your friend to do the same thing.
7. Write a reflection report in 100 words about the role cryptography is playing in ensuring individual privacy in banking websites.

(Refer to <http://www.pa.msu.edu/reference/pgpdoc1.html> and

<http://www.pa.msu.edu/reference/pgpdoc2.html>, or any document about PGP/GPG)

**Scoring**

|  |  |  |
| --- | --- | --- |
| **Type** | **Score** | **Description** |
| **Content** | | |
| 4 keys being generated | 5 | Keys of different sizes should be generated, contents of keys included, and size estimated. Discuss why generation of different size of keys take different time. |
| File encryption | 5 | File encryption with one key and results included with observation. |
| Large file encryption | 5 | Analysis and observation of encryption time for large files, presentation of command used to generate file containing random data. |
| ASCII format | 5 | Need for keys and encrypted files to be in ASCII format |
| Key exchange for cryptography | 5 | Observation of key exchange, encryption and decryption of the file shown with screen shots of results |
| Reflection on use of cryptography | 10 | Role of cryptography in banking websites to ensuring right to privacy |
| Subtotal: | **35** | Subtotal for content |
| **Presentation** | | |
| Spelling and Grammar | 5 | The presentation’s content is appropriately written in English, with no spelling errors and grammar issues. |
| Presentation and Style | 5 | The report is well presented, with diagrams, headings, tables and other visual aids. |
| References | 5 | The report contains appropriate references and referencing style. |
| Subtotal: | **15** | Subtotal for presentation |
| Total: | **50** |  |