

**FACULTY OF INFORMATICS**

**COURSEWORK COVERSHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **SUBJECT’S INFORMATION:** | | | |
| Subject: | CSCI368 Network Security | | |
| Session: | February 2020 | | |
| Programme / Section: | BCS | | |
| Lecturer: | **Mohamad Faizal Alias** | | |
| Coursework Type  *(tick appropriate box)* | ❑ Individual Assessment | | |
| Coursework Title: | Assessment 2 | Coursework Percentage: | 14% |
| Hand-out Date: | Week 6 | Received By :  (signature) |  |
| Due Date: | Week 12 | Received Date : |  |
| **STUDENT’S INFORMATION:** | | | |
| Student’s Name & ID: |  |  |  |
| Contact Number / Email: |  |  |  |
| **STUDENT’S DECLARATION** | | | |
| By signing this, I / We declare that:   1. This assignment meets all the requirements for the subject as detailed in the relevant Subject Outline, which I/ we have read. 2. It is my / our own work and I / we did not collaborate with or copy from others. 3. I / we have read and understand my responsibilities under the University of Wollongong’s policy on plagiarism. 4. I / we have not plagiarised from published work (including the internet). Where I have used the work from others, I / we have referenced it in the text and provided a reference list at the end of the assignment.   I am / we are aware that late submission without an authorised extension from the subject co-ordinator may incur a penalty. *(See your subject outline for further information).* | | | |
| Name & Signature: |  |  |  |

------------✂ -------------------✂ ------------------✂ -------------------✂ --------------------✂ ---------------------✂ --

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subject: | CSCI368 Network Security | | Session: | February 2020 |
| Programme / Section: | BCS | | Lecturer: | **Mohamad Faizal Alias** |
| Coursework Type:  (Tick appropriate box) | ❑ Individual Assessment | | | |
| Coursework Title: | Assessment 2 | Coursework Percentage: | | 14% |
| Hand-out Date: | Week 6 | Received By:  (Signature) | |  |
| Due date: | Week 12 | Received Date: | |  |
| **STUDENT’S INFORMATION:** | | | | |
| Student’s Name & ID: |  |  | |  |
| Contact Number / Email: |  |  | |  |

**COURSEWORK SUBMISSION RECEIPT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Assessment Criteria** | | **Total Marks** | **Given Marks** |
|  | **Part 1:** Online Quiz 3 – PKI (Must be completed within **Week 6**) | 2 |  |
|  | **Part 2: Secret File Server System (Submission by Week 12)** | 8 |  |
|  | 1. Authentication Server code 2. Client and creating account code and KeyGen 3. IDEA encryption and OFB Mode code 4. FTP file server, connection code, Upload and Download 5. Report   **Note**: Presentation on Week 14 required | 1. /2 2. /2 3. /2 4. /3 5. /1 |  |
|  | | **10** |  |
|  | | **Penalty** |  |
| Marked by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_ | | **Final Mark (10 %)** |  |
| **Lecturer’s Comments** | | | |
|  | | | |
| **Penalty for late submission:** | | | |
| 1 day – minus 20% of total mark awarded  2 days – minus 50% of total mark awarded  3 days – 0 mark for this piece of coursework | | | |

**University of Wollongong**

**CSCI368 NETWORK SECURITY**

**February 2020**

**Individual Assessment 2 (10 %)**

**Aims**

This assignment consists of **TWO** parts. Part 1 consists of an Online Quiz 3 covering topic of Public Key Infrastructure.

Where by Part 2 is a program development for Secret File Server system

**Objectives**

On completion of this assignment you should be able to:

* Understand Cloud Computing and Cloud Security
* Understand the Public Key Infrastructure covering Key Management, Digital Certificates and Key Distribution
* Applying network programming.
* Applying Cryptographic techniques such as Key Generator, Hashing, block cipher and secured file transfer (Programming)

**Part 1 – Online Quiz 3 – PKI (2%) – Week 6**

* Quiz 3 is an online quiz on Moodle which consist of 10 MCQs. You are given only 20 minutes to complete the quiz.
* The coverage for this quiz is on Chp04 – Public Key Infrastructure.
* Make sure you have done necessary reading before attempting this quiz.
* Quiz will be open on Week 6 Monday and close by Week 5 Sunday.

**Part 2 – Secret File Server System**

**Aims**

This Part 2 assignment aims to establish a basic familiarity with an authentication system, encryption of block ciphers and file transfer with confidentiality.

**Part 2 Objectives**

The assignment involves the following tasks:

* Implementation of a working prototype of secret file server system.
* Socket programming.
* Security programming including block ciphers, hashed password file and authentication server

On completion of this assignment you should be able to:

* Understand advanced authentication systems.
* Understand block cipher and hashing during authentication and file transfer
* Write security code for communications in computer networks.
* Write socket code.

**Specifications**

Write a C++ socket program to implement a working prototype of secret file server system

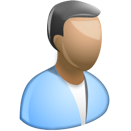
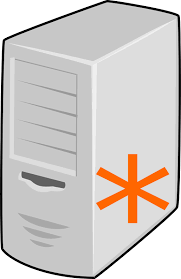
Configuration of either internal or external (cloud service) FTP server

Use of a new library: ChilKat FTP Reference (library). Refer notes at the end of the specification.

**SECRET FILE SERVER SYSTEM**

**Planning:**

|  |  |  |
| --- | --- | --- |
| **Client Program** | **Authentication Server** | **FTP File Server** |
| **Spec.**  Own program With IDEA Key 1  Crypto++ library  C++ FTP library  Reverse IDEA Key 2 to make IDEA Key 3 to be used during upload/download to FTP server. | **Spec.**  Own program with IDEA Key 1  Store: User Account with IDEA Key 2  Crypto++ library  C++ FTP library | **Spec.**  Windows 10 FTP Server configuration (minimum)  Alternatively, cloud FTP server |

** **

Windows 10 FTP server or Cloud FTP Server

****

Authentication Server

User & Client Program

**Requirements:**

1. **Execution and Network**
2. Windows 10 FTP server is a configure server with IP and FTP service. It should be readily starts and with a fixed account and password (Single Administrator account). Alternatively, you may create account on free FTP cloud service, but read carefully the policy for free account. (Example Hostinger.my or any other FTP service)
3. Authentication server (AS) is your own program that handles user account management and authentication process during client program logon.
4. AS stores, all user accounts, Hash of the user’s password in a secured file and randomly generated Key (in user account file).
5. The user account file is a standard text file but all user accounts, hash of password, key and date register are encrypted using **IDEA encryption with OFB Mode. The key (IDEA Key1) is hardcoded in the AS program itself.**
6. During startup of AS, it has its own IP address and opened port number (entered by the admin during AS execution) for client program to connect.
7. During this time, entry for IP address of FTP server, server name (if required), admin ID and password must be entered.
8. This information later will be used by AS to pass securely to the client program over the network.
9. **Account Creation**
10. Using the Client program, a user can register his/her account and decide a password.
11. The password should be between 8 to 12 characters long.
12. During account creation, AS also randomly generate 16 characters long key (**IDEA Key 2**). This Key is uniquely assigned to each user.
13. The user account, hash of password **(SHA-1 hashing)**, **IDEA Key 2**, registered date is securely stored by AS in a file mentioned above (in A.3).
14. With the client program, a user also can change his/her own password at later time. But the **IDEA Key 2** remain the same.
15. User account only **can be use after 24hours from the date created** for FTP operation. Use account created date to verify.
16. AS program will also update the random **IDEA Key 2** assigned to each user’s account every 2 months, based on registered date stored.
17. **Authentication**
18. Using the client program, any user can request to connect to the FTP server via AS.
19. AS is required to authenticate the user login based on the user account file already exists.
20. The password entered by the user should be hash **(SHA-1)** and compared both user ID and hash of the password with the user account file already exists.
21. Upon authenticated by the AS, the **client program should receive the FTP server detail and IDEA Key 2 (uniquely assigned to the user) encrypted using OFB IDEA encryption with IDEA Key 1.**
22. The **IDEA key (IDEA Key 1)** used for both client program and AS can be hard-coded in both programs.
23. **FTP file server setup (No programming requried)**
24. FTP server is configured in a standard Windows 10 PC having one admin account and password. (Alternative, Cloud FTP server)
25. All FTP upload and download is managed by only this account. Possibly one folder.
26. The information regarding FTP server need to be entered during AS startup as mentioned in A.6 above.
27. FTP server handle upload and download of file between client program and itself.
28. **The file received by FTP server is already a secured file. Encrypted and decrypted by the client program.**
29. The client program is using **IDEA encryption with OFB** to encrypt and decrypt the file before it is uploaded to the FTP server.
30. The key used by the IDEA encryption (**IDEA Key 3**) is reverse character of **IDEA Key 2** received from AS during the login process and after authentication satisfied.
31. As mentioned, the encryption and decryption of file is handled by client program and using **IDEA Key 3** (the reverse of IDEA Key2 stored in AS and received during authentication between client and AS).
32. During file download, the client program should decrypt the file received from FTP server using similar process in D.7 and D.8 above.
33. File should use the same extension before and after encryption/decryption.
34. **Secure client upload/download to/from FTP server**
35. After authentication of user account via client program. Communication is established between client program and FTP server directly without intervention from AS.
36. Secured file upload/download process can be initiated by the user via client program. Refer D.6 to D.10 above.
37. Client program in charge of encryption and decryption of the file to create the original file with appropriate extension.
38. For our program simulation and testing, ensure that file of **\*.docx, \*.png, \*.jpg, \*.txt and \*.pdf** are encrypted and decrypted correctly. These should be reported.

**References:**

1. C++ File Upload: <https://www.example-code.com/vcpp/ftp_upload.asp>
2. C++ File Download: <https://www.example-code.com/cpp/ftp_download.asp>
3. ChilKat FTP Reference (library): <https://www.chilkatsoft.com/refdoc/vcCkFtp2Ref.html>

**Warning**: ChilKat does not give away the library for free anymore. You have limited time of using it. Please refer to his website for latest update.

1. How to setup FTP with Windows 10: <https://www.windowscentral.com/how-set-and-manage-ftp-server-windows-10>

**Note:**

* You may use any other C++ library deemed suitable for FTP apart from the above suggestion. But FTP server remains on Windows 10 PC or Cloud FTP service.
* If you would like to host the FTP server on other platform, please get permission from your lecturer.

**Files to be submitted:**

* All source code
* readme (text file)
* A report in pdf format containing some screen captures about the whole execution, and explanation of the working system.
* Complete test results of different file extension during uploading and downloading (encrypt/decrypt)

Generate a zip file named <yourname><assign2>.zip that includes all the above files to be submitted. Put your name and student number in all source codes.

**Submission**

This assignment should be submitted electronically via the assignment submission link on Moodle:

Comments in code files should be concise. A header should give your information (including name, student ID) and briefly summarize the contents of the file - identifying purpose of program, listing classes etc.

Classes may have brief header comments if these are considered necessary.

Individual functions should only require comment if they are complicated or result in non-obvious side effects etc.

The code that does not compile or/and failure of client/server connection will receive a zero.

**Note**: A presentation session will be prepared for you to show case your system in Week 14

**Late Submission:**

Penalty is 25% deduction per day.

**Plagiarism**

A plagiarised assignment will receive a zero mark and be penalised according to the university rules. Plagiarism detection software will be used.