Assignment Guidance and Front Sheet

This front sheet for assignments is designed to contain the brief, the submission instructions, and the actual student submission for any WMG assignment. As a result the sheet is completed by several people over time, and is therefore split up into sections explaining who completes what information and when. Yellow highlighted text indicates examples or further explanation of what is requested, and the highlight and instructions should be removed as you populate 'your' section.
This sheet is only to be used for components of assessment worth more than 3 CATS (e.g. for a 15 credit module, weighted more than 20%; or for a 10 credit module, weighted more than 30%).

To be completed by the student(s) prior to final submission:
Your actual submission should be written at the end of this cover sheet file, or attached with the cover sheet at the front if drafted in a separate file, program or application.

Student ID or IDs for group work	**2286790**

To be completed (highlighted parts only) by the programme administration after approval and prior to issuing of the assessment; to be consulted by the student(s) so that you know how and when to submit:

Date set	13th January 2023
Submission date (excluding extensions)	13th February 2023 12:00pm (UK Time)
Submission guidance	Submit Electronically to Tabula
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late. For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

To be completed by the module owner/tutor prior to approval and issuing of the assessment; to be consulted by the student(s) so that you understand the assignment brief, its context within the module, and any specific criteria and advice from the tutor:

Module title & code	Management of Cryptosystems (WM9C5-15)
Module owner	Henry Caushi
Module tutor	Henry Caushi
Assessment type	Report
Weighting of mark	100%

Assessment brief
Please see below

Word count	Described below
Module learning outcomes (numbered)	• Critically analyse the properties of cryptographic functions such as symmetric/asymmetric encryption systems and hashes • Evaluate competing cryptographic techniques in the solution of well defined cyber problems. • Design and simulate cryptosystems to meet desired cyber security outcomes • Critically analyse the properties of cryptographic protocols.
Learning outcomes assessed in this assessment (numbered)	As above
Marking guidelines	Generally indicated within specification
Academic guidance resources	All queries to be directed to the PMA channel

Contents

Executive Summary

This report analyses the existing infrastructure at the University of Varvick and offers a solution to all the data security and cryptographic needs. By implementing single sign-on, the university hopes to integrate all service logins and enable access to all services through a single login. Additionally, The University wants to expand its one cloud to store all the sensitive data like financial records, exam papers and collaborators private research data and wishes to access them remotely.

As a cyber security developer, I propose to use Kerberos Single-Sign on with Multi-Factor Authentication along with Role Base Access Control and encryption of data at rest. In addition to being highly fault tolerant, it is also highly secure and compatible with a variety of platforms. Using additional layer of authentication will comply to the intention of securing sensitive data.

Introduction

The University of Varwick needs to redesign cryptographic procedures and security, while expanding its OneCloud instance to store sensitive data used by various systems. This report outlines a cryptographic simulation for the university. The plan also considers the University's requirement for a Single Sign-On (SSO) system that would enable users to access online services with just a single login, Role based access control and Encryption of data. The suggested remedy strives to protect data privacy, availability, and integrity while adhering to PSD2, CCPA, and GDPR rules.

Scope

The scope of this report includes the 5 services (Troodle, Fabula, MyVarvick, Courses@Varvick and conker) along with OneCloud server and User groups.

Methodology

- Identify all the data storage and movement patterns- Looking into the existing data transfer mechanisms and storage systems.
- Conduct a risk assessment- Identify the possible Cyber-Risks to the existing infrastructure and find ways to mitigate those risks.
- Implement the encryption algorithms for sensitive data- It is necessary to perform secure key encryption and storage along with file and disc level encryption. Given that the entire system should comply with PSD2, GDPR, and CCPA
- Implement Authentication Protocol and Multi Factor Authentication- Implement the SSO using suitable authentication protocol and add multi factor authentication for additional security.
- Implement Role Based Access Control – Provide access to different users according to their roles.
- Monitor and Maintain- Regular Monitoring and logging to ensure stability, availability and better incident response.

Findings

- Currently The University stores all the data of Fabula, Conker, MyVarwick, Troodle, and Courses@Varwick data on-premises. They need to redesign all the cryptographic communication and data storage practices.
- University has implemented RBAC (Role Base Access Control), but needs to increase it's security and encryption of data at rest must be done.
- Reportedly, University is cyber-security conscious and needs to encrypt the sensitive data at rest and must be accessed by authorised personnel only.
- University needs SSO for accessing multiple servers using a single login. And to increase a layer of security, Kerberos can be modified to perform 2FA in the form of OTP authentication.
- Key Management and storage must be redesigned.
- The solution should be compliant to PSD2, GDPR, and CCPA.

Proposed System

Kerberos Authentication System- Kerberos is a network authentication system. It is a client-server authentication protocol in which access to the services are granted only if the user is authorised using cryptographic techniques and trusted third party server like KDC (Key Distribution Server). The server will ensure that every transmission is encrypted and provide central authentications for all the services.

The use of Kerberos is advantageous because it is scalable and broadly supported by various operating systems. This system will have many user groups and should be highly available at all times. A protocol that performs mutual authentication will be the best option because the university cannot tolerate any threat to the sensitive and confidential data stored at rest. It is also an open protocol, meaning there are no licencing fees and remote access is possible.

Additionally, there is no password exchange in Kerberos. To verify the private key, the key is hashed and sent securely to the server. By doing this, attacks such as phishing, identity theft, brute force, and others can be prevented.

Kerberos has three entities:

1. Authentication Server- The authentication server is responsible for user's secret key validation, along with two factor authentication.
2. Ticket Granting Server- Ticket Granting Server is responsible for issuing service tickets to the users.
3. Service Server- Service server is the actual server that will provide access to services.

Kerberos has four stages:

1. The user requests logins using username and password, the Kerberos Ticket granting server will generate ticket granting server ticket and send it to authentication server .
2. The Authentication Server will send an OTP to the user and verify the OTP. If the OTP is verified, Ticket granting ticket is sent to the user to access Ticket granting Server .
3. The user will send the TGT issued to the TGT server, and it verifies the TGT and issues a service ticket. The service ticket is sent to the user. The user then sends the service ticket to the requested service server.
4. The service server will verify the service ticket, check lifetime, and grant access to the requested lifetime.
5. The user can access different services by requesting service ticket to different service server.

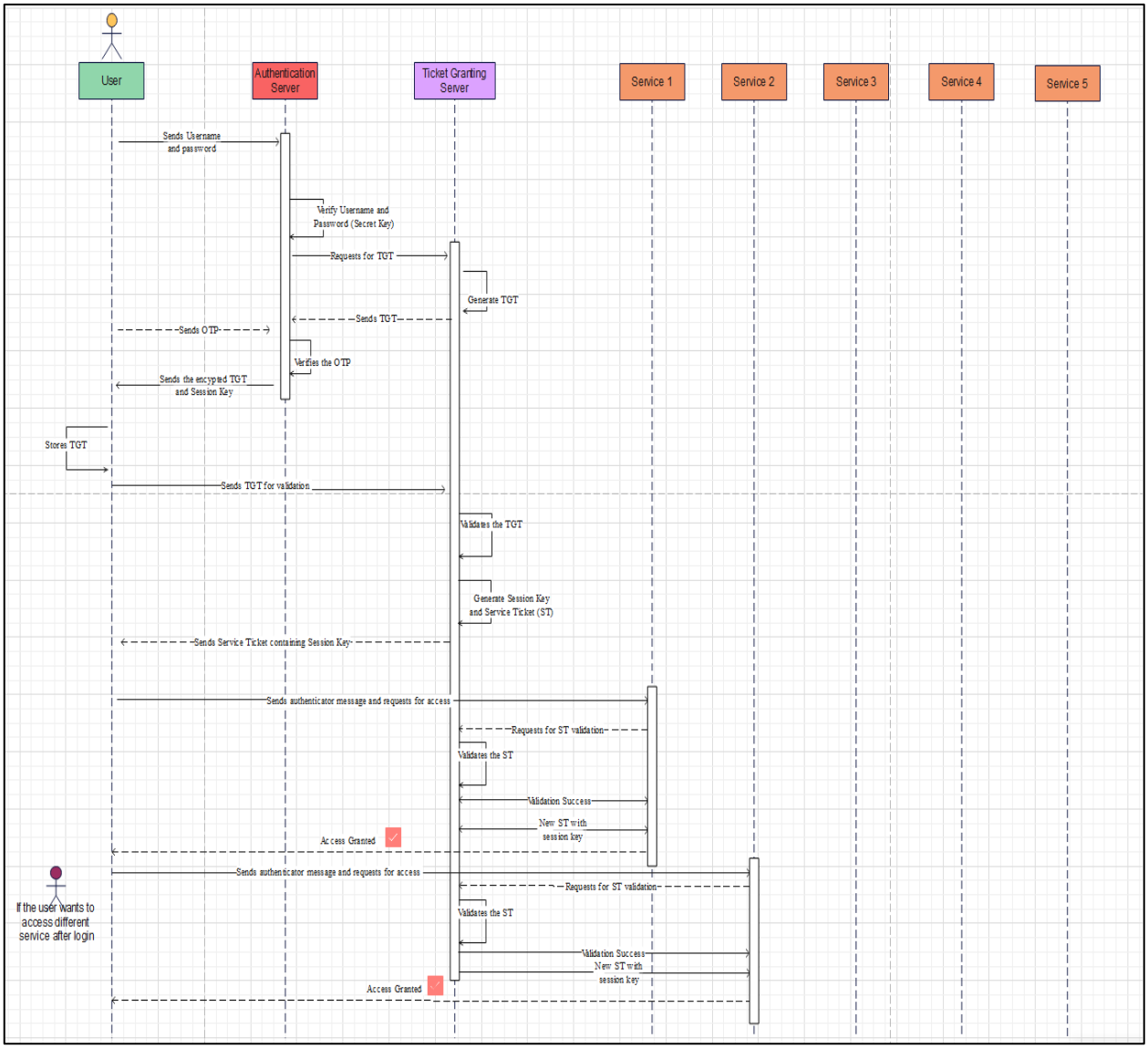
Role Based Access Control – The university already has RBAC and can improve data at rest. OneCloud supports file and disk level encryption which will keep the sensitive data safe. AES (Advanced Encryption Standard) is used to encrypt data at rest. AES is symmetric key algorithm which is fast and efficient for encrypting and decrypting large amount of data. Additionally, it is resilient to cyber-attacks as the key length 256 bits, that is difficult to crack. After the data is encrypted twice, the end keys are stored in Key Management Server. This will ensure that the data is secure on cloud. Whenever a user group request access to specific server, they get different website views for everyone. The proposed SSO will be integrated with the existing RBAC. The data transfer between the cloud server and the services is secured by TLS (Transport Layer Security).

Sr. No.	Roles	Troodle	Fabula	Courses@Varwick	Conker	MyVarwick	OneCloud
1	Students	☑	☑	☑	☑	☑	☑
2	Staff	☑		☑	☑		☑
3	Faculty		☑				☑
4	Finance Team				☑		☑
5	Partner Company						☑
6	Welfare Team						☑

Redesign Security and Cryptographic Practices – Previously the data for all the web servers along with MyVarvick application server was stored on-premises. That would cost a lot of money and maintenance. Migrating to cloud will not only reduce the efforts of maintain and securing the data, but also provide backups. Also, all the data can now be secure and accessed from anywhere in the world. The provided solutions will ensure Confidentiality, integrity and availability of sensitive data. Hashing the cryptographic keys will ensure that the keys are secure.

Sequence Diagram

The following sequence diagram shows interaction between User and all the services.



Narrative Description

1. User logins using Username and password and requests for Ticket – Granting Service.
2. The Kerberos AS verifies the received client's secret key with the database.
3. The TGT sends generates and send the ticket to AS.
4. The AS will generate OTP and send it to the user.
5. The user will send the received OTP to the AS.
6. The AS will validate the OTP and send the TGT .
7. User will send the TGT to the TGS.

8. TGS will create a service ticket for the requested service.
9. The service ticket is sent to the user.
10. The user will present the service ticket to the service.
11. The service will verify the ticket and grant access.

Conclusion

The proposed system will meet all the requirements mentioned by the university with lowest efforts, complexity but highest security. The solution includes on-cloud encryption, decryption, secure key management, RBAC (Role Base Access Control), 2FA (Two Factor Authentication), and compliant to GDPR, PSD2, CCPA.