School of Computing Technologies

**INTE2401/2402/2691 Cloud Security**

Assignment 2

|  |  |
| --- | --- |
| RMIT_icon_Industry_connections_Red_RGB.png | **Assessment Type:** Individual assignment; no group work. Submit online via Canvas→Assignments→Assignment 2.  Marks awarded for meeting requirements as closely as possible. Clarifications/updates may be made via announcements/relevant discussion forums. |
| RMIT_icon_add_an_event_Red_RGB.png | **Due date: Week 8, Sunday the 4th May 2025 11:59pm**  As this is a major assignment in which you demonstrate your understanding, a university standard late penalty of 10% per each working day applies for up to 5 working days late, unless special consideration has been granted. |
|  | **Weighting: 35 marks (Contributes 35% of the total Grade)** |

1. **Overview**

The objective of Assignment 2 is evaluating your knowledge on the topics covered mainly in Lecture 2 to 8. Topics include SHA-3, HMAC, Kerberos, and Security Protocols for Cloud Computing. However, topics covered in Lecture 1 are required as prerequisite. Assignment 2 will focus on developing your abilities in application of knowledge, critical analysis and decision making. Assignment 2 contains several problems related to the topics mentioned above. You are required to prepare your answers and upload them as a zipped (compressed) file in CANVAS.

In this assignment, there are 5 (five) questions related to AWS.

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3 uses checksum values to verify the integrity of data that you upload or download. You can choose a hash function as the checksum algorithm to use when uploading, copying, or batch copying your data. **SHA-3 (Secure Hash Algorithm 3)** is the latest member of the Secure Hash Algorithm family of standards, released by NIST on August 5, 2015. The first question of this assignment is about SHA-3. You are expected to hash your personal information in one round of SHA-3. Through this question, you are expected to understand the hash process of SHA-3 in details.

Question 2 is on **Signing AWS Requests with Signature Version 4.** When you send HTTP requests to AWS, you need to sign the requests so that AWS can identify who sent them. You sign requests with your AWS access key, which consists of an access key ID and secret access key. The signing process helps secure requests in the following ways: verify the identity of the requester, protect data in transit, and protect against potential replay attacks. In this question, you are required to use AWS Signature Version 4 to generate a signature on a given string. Through this question, you are expected to understand the detail signature generation and verification process of AWS Signature Version 4.

Question 3 is about **Kerberos authentication in AWS.** In AWS,you can use Kerberos authentication to authenticate users when they connect to your MySQL DB instance. The DB instance works with AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) to enable Kerberos authentication. When users authenticate with a MySQL DB instance, authentication requests are forwarded. Forwarded requests go to the domain directory that you create with AWS Directory Service. Keeping all of your credentials in the same directory can save you time and effort. With this approach, you have a centralized place for storing and managing credentials for multiple DB instances. Using a directory can also improve your overall security profile. In this question, you are required to implement Simplified Kerberos for AWS. Through the question, you are expected to understand how Kerberos authentication is used to authenticate a user when he connects to your MySQL DB instance in AWS.

Question 4 is about **AWS Site-to-Site VPN** based on Diffie-Hellman key establishment. An AWS Site-to-Site VPN connection connects your Virtual Private Cloud (VPC) to your data centre. Amazon supports Internet Protocol Security (IPSec) VPN connections. Data transferred between your VPC and data centre routes over an encrypted VPN connection to help maintain the confidentiality and integrity of data in transit. Internet Key Exchange (IKEv2) is the protocol used to set up a security association (SA) in the IPSec protocol suite. IKEv2 uses a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. The question has three parts. In the first part, you are expected to implement the Diffie-Hellman key exchange protocol for AWS Site-to-Site VPN. In the second part, you are expected to perform a man-in-the-middle attack to the Diffie-Hellman key exchange protocol. In the last part, you are expected to propose an improved key exchange protocol which is able to overcome the man-in-the-middle attack.

The last question is on **Secure Socket Layer (SSL) Handshake Protocol.** Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client - typically a web server (website) and a web browser. AWS Certificate Manager from Amazon Web Services (AWS) takes care of deploying certificates to help you enable SSL/TLS for your website. Assume that AWS Certificate Manager issues you a SSL certificate and you have installed the certificate in your website hosted on AWS. When a client browses your website, suppose the client will run a SSL handshake protocol with ephemeral public key with your website to establish an encrypted link between the client and your website. In this question, we are expected to demonstrate your understanding how SSL handshake protocol with ephemeral public key work and analyse client authentication, server authentication, and forward security of the SSL handshake protocol.

Develop this assignment in an iterative fashion (as opposed to completing it in one sitting). You should be able to start preparing your answers immediately after Lecture-5 (in Week-5). At the end of each week starting from Week-5 to Week-8, you should be able to solve at least one question.

If there are questions, you may ask via the relevant Canvas discussion forums in a general manner.

1. **Learning Outcomes**

This assessment is relevant to the following Learning Outcomes:

* understand how AWS applies hashing techniques, digital signature, key management, and security protocols to achieve cloud security.
* discuss various types of confidentiality, authentication and data integrity mechanisms in cloud computing.
* analyze the strength and limitations of security protocols for cloud computing.
* design and implement security mechanisms and protocols.

1. **Submission**

You must follow the following special instructions:

* You must use the values provided in the questions.
* Hand-written answers are not allowed and will not be assessed. Compose your answers using any word processing software (e.g. MS Word).
* You are required to show all of the steps and intermediate results for each question.
* Upload your solutions as a single PDF or Word document together with programming codes in CANVAS.

This assessment will determine your ability to:

* Follow requirements provided in this document and in the lessons.
* Independently solve a problem by using security concepts taught over the first four weeks of the course.
* Meeting deadlines.

After the due date, you will have 5 business days to submit your assignment as a late submission. Late submissions will incur a penalty of 10% per day. After these five days, Canvas will be closed and you will lose ALL the assignment marks.

1. **Assessment details**

Please ensure that you have read **Section 1** to **3** of this document before going further. Assessment details (i.e. question Q1 to Q5) are provided in the **next page**.

**Q1. Cloud Data Checksum with SHA-3 (Marks: 1+1+1+1+1=5)**

|  |
| --- |
| Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3 uses checksum values to verify the integrity of data that you upload or download. You can choose a hash function as the checksum algorithm to use when uploading, copying, or batch copying your data. SHA-3 (Secure Hash Algorithm 3) is the latest member of the Secure Hash Algorithm family of standards, released by NIST on August 5, 2015. SHA-3 is based on a novel approach called sponge construction. Sponge construction is based on a wide random permutation, and allows inputting ("absorbing" in sponge terminology) any amount of data, and outputting ("squeezing") any amount of data, while acting as a pseudorandom function with regard to all previous inputs. This leads to great flexibility. In this question, you are expected to hash your personal information in the first round of SHA-3 as shown in Figure 1.    **Figure 1. SHA-3 Round Function**  Assume that you are using SHA-3 to calculate the checksum of the first 200 bits of the ASCII codes of your personal information, including your real name, student ID, email address, your program, your courses …. (Note that the format does not matter as long as we can identify you).   1. What is the output of mapping in the first round? 2. What is the output of mapping in the first round? 3. What is the output of mapping in the first round? 4. What is the output of mapping in the first round? 5. What is the output of mapping in the first round?   **Note:** Please provide your answers in 5x5 matrixes with entries in Hex. |

**Q2. Signing AWS Requests with Signature Version 4 (Marks: 1+1+1+1+1=5)**

|  |
| --- |
| When you send HTTP requests to AWS, you need to sign the requests so that AWS can identify who sent them. You sign requests with your AWS access key, which consists of an access key ID and secret access key. The signing process helps secure requests in the following ways: verify the identity of the requester, protect data in transit, and protect against potential replay attacks. Creating a signed request includes 3 steps: (1) create a string to sign for Signature Version 4; (2) calculate the signature for AWS Signature Version 4; (3) add the signature to the HTTP request. **AWS Signature Version 4** is built on HMAC-SHA256 as shown in Figure 2.  A picture containing clock  Description automatically generated  **Figure 2. HMAC-SHA256 (k, m)**  Suppose that a string to sign is as follows:  AWS4-HMAC-SHA256  20250415M123600Z  20250415/us-east-1/iam/aws4\_request  f536975d06c0309214f805bb90ccff089219ecd68b2577efef23edd43b7e1a59  Assume that kSecret = **your student ID**/K7MDENG+bPxRfiCYEXAMPLEKEY.   1. Compute kDate = HMAC("AWS4" + kSecret, Date), where Date = 20250415; 2. Compute kRegion = HMAC(kDate, Region), where Region = us-east-1; 3. Compute kService = HMAC(kRegion, Service), where Service = iam; 4. Compute kSigning = HMAC(kService, "aws4\_request"); 5. Compute the signature = HexEncode(HMAC(kSigning, string to sign))   **Note:** Please use SHA256 <https://emn178.github.io/online-tools/sha256.html> in HMAC-SHA256.  Please your real student ID.  Please refer to <https://docs.aws.amazon.com/general/latest/gr/sigv4-calculate-signature.html> |

**Q3. AWS Kerberos Authentication (Marks: 2+2+2+2+2=10)**

|  |
| --- |
| In AWS, you can use Kerberos authentication to authenticate users when they connect to your MySQL DB instance. The DB instance works with AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) to enable Kerberos authentication. When users authenticate with a MySQL DB instance, authentication requests are forwarded. Forwarded requests go to the domain directory that you create with AWS Directory Service. Keeping all of your credentials in the same directory can save you time and effort. With this approach, you have a centralized place for storing and managing credentials for multiple DB instances. Using a directory can also improve your overall security profile. In this question, you are required to implement Simplified Kerberos for AWS as shown in Figure 3.    **Figure 3. Simplified Kerberos**   1. Implement AES-128 encryption and decryption algorithms in CBC mode. 2. Assume C=your first name, S=your surname, KC=MD5(C, your student ID), KS=MD5(S, your student ID), Lt=8 hours, nC=MD5(C), 3. implement each step of Phase 1 of Simplified Kerberos using AES-128 in (1) 4. implement each step of Phase 2 of Simplified Kerberos using AES-128 in (1) 5. What is the ticket (Hex numbers) in your implementation? What is the authenticator (Hex numbers) in your implementation? 6. Please explain how the user can be authenticated by the server and how the server can be authenticated by the user in the protocol.   **Note**: Please use MD5 <https://emn178.github.io/online-tools/md5.html>  Please submit your codes for (1) and (2).  Please use the current time as the timestamp ts in your implementation.  You can randomly choose any 128-bit KC,S and any 128-bit session key sk in your implementation. |

**Q4. AWS Site-to-Site VPN based on Diffie-Hellman Key Establishment (Marks: 2+2+2+2+2=10)**

|  |
| --- |
| An AWS Site-to-Site VPN connection connects your Virtual Private Cloud (VPC) to your data centre as shown in Figure 4. Amazon supports Internet Protocol Security (IPSec) VPN connections. Data transferred between your VPC and data centre routes over an encrypted VPN connection maintain the confidentiality and integrity of data in transit. Internet Key Exchange (IKEv2) is the protocol used to set up a security association (SA) in the IPSec protocol suite. IKEv2 uses X.509 certificates for authentication ‒ either pre-shared or distributed and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.  A screenshot of a cell phone  Description automatically generated  **Figure 4. AWS Site-to-Site VPN**  The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. In this question, you are required to implement the Diffie–Hellman key exchange protocol (Group 2) between your VPC and your data centre.  For the Diffie-Hellman key exchange protocol, assume  **--**  p=178011905478542266528237562450159990145232156369120674273274450314442865788737020770612695252123463079567156784778466449970650770920727857050009668388144034129745221171818506047231150039301079959358067395348717066319802262019714966524135060945913707594956514672855690606794135837542707371727429551343320695239  g=174068207532402095185811980123523436538604490794561350978495831040599953488455823147851597408940950725307797094915759492368300574252438761037084473467180148876118103083043754985190983472601550494691329488083395492313850000361646482644608492304078721818959999056496097769368017749273708962006689187956744210730  --   1. Implemenent 160-bit random number geneator and secure hash algorithm SHA1; 2. Use a Crypto Library to implement the modular exploentiation algorithm for larger integers and use your implementation to output y=gx(mod p), where x=SHA1(your student ID). 3. After randomly genetating 160-bit a and 160-bit b, output (A, gA(mod p)) and (B, gB(mod p)) and the secret key gAB (mod p) established between your VPC (named by your first name) and your data centre (named by your surname) by the Diffie-Hellman key exchange protocol, where A=SHA1(a, your first name) and B=SHA1(b, your surname). 4. Can you perform a **Man-in-the-Middle** **Attack** to the Diffie-Hellman key exchange protocol? If so, show attacking steps. 5. How does IKEv2 overcome the **Man-in-the-Middle** **Attack**?Show steps.   **Note**: Please submit your codes, computation results, security analysis and secure protocol. |

**Q5. SSL Handshake Protocol (Marks: 1+1+1+1+1=5)**

|  |
| --- |
| AWS Certificate Manager from Amazon Web Services (AWS) takes care of deploying certificates to help you enable SSL/TLS for your website. Assume that AWS Certificate Manager issues you a SSL certificate and you have installed the certificate in your website hosted on AWS. When a client browses your website, suppose the client will run a SSL handshake protocol with ephemeral public key with your website to establish an encrypted link between the client and your website as shown in Figure 5.  *image18.png*  **Figure 5. SSL Handshake Protocol**  In the certificate of your website, if 2048-bit RSA public keys are  n=  e=(10001)16  If your private signing key is  d=   1. Choose your ephemeral public key with 1024 bits and set e as the largest prime factor of your student number. 2. What is the ServerKeyExchange message (Hex numbers) in Figure 5? 3. If Pre\_Master\_Secret is SHA384(your real email address), where the hash function is SHA384 (<https://emn178.github.io/online-tools/sha384.html>), what is the ClientKeyExchange message (Hex number) in Figure 5? 4. Analyse client authentication and server authentication of the handshake protocol. 5. Analyse the forward security of the handshake protocol.   Hint: Compute modular exponentiations and inverse with online tool at <https://www.boxentriq.com/code-breaking/modular-exponentiation>.  <https://www.boxentriq.com/code-breaking/modular-multiplicative-inverse> |

1. **Academic integrity and plagiarism (standard warning)**

Academic integrity is about honest presentation of your academic work. It means acknowledging the work of others while developing your own insights, knowledge and ideas. You should take extreme care that you have:

* Acknowledged words, data, diagrams, models, frameworks and/or ideas of others you have quoted (i.e. directly copied), summarized, paraphrased, discussed or mentioned in your assessment through the appropriate referencing methods,
* Provided a reference list of the publication details so your reader can locate the source if necessary. This includes material taken from Internet sites.

If you do not acknowledge the sources of your material, you may be accused of plagiarism because you have passed off the work and ideas of another person without appropriate referencing, as if they were your own.

RMIT University treats plagiarism as a very serious offence constituting misconduct. Plagiarism covers a variety of inappropriate behaviors, including:

* Failure to properly document a source
* Copyright material from the internet or databases
* Collusion between students

For further information on our policies and procedures, please refer to the [University website.](https://www.rmit.edu.au/students/student-essentials/rights-and-responsibilities/academic-integrity)

1. **Assessment declaration**

When you submit work electronically, you agree to the [assessment declaration.](https://www.rmit.edu.au/students/student-essentials/assessment-and-exams/assessment/assessment-declaration)

1. **Rubric/assessment criteria for marking**

All of the computations must be correct and only provided values must be used. Instructions must be followed.

|  |  |  |
| --- | --- | --- |
| **Criteria**  The characteristic or outcome that is being judged. |  | **Total** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Question 1**  Cloud Data Checksum with SHA-3 | **Questions (1)-(5) are answered correctly.**  **Step-by-step processes are shown with detail computations.**  **All of the computations are shown correctly in detail.** | Any 4 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations.  The computations in the 4 questions are shown correctly in detail. | Any 3 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations.  The computations in the 3 questions are shown correctly in detail. | Any 2 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations.  The computations in the 2 questions are shown correctly in detail. | Any one of questions (1)-(5) is answered correctly.  Step-by-step processes are shown with detail computations.  The computations in the 1 question are shown correctly in detail. | Answer is not correct  Or  Not answered | 5 Marks |
| **5 Marks** | 4 Marks | 3 Marks | 2 Mark | 1 Mark | 0 Marks |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Question 2**  Signing AWS Requests with Signature Version | **Questions (1)-(5) are answered correctly.**  **Step-by-step processes are shown with detail computations.**  **All of the computations are shown correctly in detail.** | Any 4 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations.  The computations in the 4 questions are shown correctly in detail. | Any 3 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations.  The computations in the 3 questions are shown correctly in detail. | Any 2 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations.  The computations in the 2 questions are shown correctly in detail. | Any one of questions (1)-(5) is answered correctly.  Step-by-step processes are shown with detail computations.  The computations in the 1 question is shown correctly in detail. | Answer is not correct  Or  Not answered | 5 Marks |
| **5 Marks** | 4 Marks | 3 Marks | 2 Mark | 1 Mark | 0 Marks |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Question 3**  AWS Kerberos Authentication | **Questions (1)-(4) are answered correctly.**  **All of the implementations and security analysis are done correctly in detail.** | Any 4 of questions (1), (2) (i), 2(ii), (3), (4) are answered correctly.  The implementations and security analysis in the 4 questions are done correctly in detail. | Any 3 of questions (1), (2) (i), 2(ii), (3), (4) are answered correctly.  The implementations and security analysis in the 3 questions are done correctly in detail. | Any 2 of questions (1), (2) (i), 2(ii), (3), (4) are answered correctly.  The implementations and security analysis in the 2 questions are done correctly in detail. | Any 1 of questions (1), (2) (i), 2(ii), (3), (4) are answered correctly.  The implementations and security analysis in the 1 question are done correctly in detail. | Answer is not correct  Or  Not answered | 10 Marks |
| **10 Marks** | 8 Marks | 6 Marks | 4 Mark | 2 Mark | 0 Marks |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Question 4**  AWS Site-to-Site VPN based on Diffie-Hellman Key Establishment | **Questions (1)-(5) are answered correctly.**  **All of the implementations and security analysis are done correctly in detail.** | Any 4 of questions (1)-(5) are answered correctly.  The implementations and security analysis in the 4 questions are done correctly in detail. | Any 3 of questions (1)-(5) are answered correctly.  The implementations and security analysis in the 3 questions are done correctly in detail. | Any 2 of questions (1)-(5) are answered correctly.  The implementations and security analysis in the 2 questions are done correctly in detail. | Any one of questions (1)-(5) is answered correctly.  The implementations and security analysis in the 1 question is done correctly in detail. | Answer is not correct  Or  Not answered | 10 Marks |
| **10 Marks** | 8 Marks | 6 Marks | 4 Mark | 2 Mark | 0 Marks |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Question 5**  SSL Handshake Protocol | **Questions (1)-(5) are answered correctly.**  **Step-by-step processes are shown with detail computations.**  **All of the computations and security analysis are shown correctly in detail.** | Any 4 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations.  The computations and security analysis in the 4 questions are shown correctly in detail. | Any 3 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations.  The computations and security analysis in the 3 questions are shown correctly in detail. | Any 2 of questions (1)-(5) are answered correctly.  Step-by-step processes are shown with detail computations.  The computations and security analysis in the 2 questions are shown correctly in detail. | Any one of questions (1)-(5) is answered correctly.  Step-by-step processes are shown with detail computations.  The computations and security analysis in the question are shown correctly in detail. | Answer is not correct  Or  Not answered | 5 Marks |
| **5 Marks** | 4 Marks | 3 Marks | 2 Mark | 1 Mark | 0 Marks |  |