|  |
| --- |
| CSEMAD MOBILE APPLICATION DEVELOPMENT  Assessment 1 –  Phase 1 |
| Due 28 MAR 2025  Students: 20219568, x  Authored by: Luke Gardiner, Richard Avery |

TASK 1 – LEAN CANVAS

1. Unencrypted message content that includes a Message Authentication Code (MAC) generated and validate using symmetrical encryption.
2. Unencrypted message content that includes a Hash Function or Digital Signature employing an asymmetrical encryption process.
3. Encrypted message content using a symmetrical or asymmetrical encryption process and including additional validation measures such as time stamping and sequence numbers.

TASK 2 –   
a) What is a Message Authentication Code

b) What is a one-way hash function? How is it different to a message authentication code?

a)

A Message Authentication Code (MAC) is a method of proving the authenticity of a transmitted message by generating and including a MAC utilising a secret key possessed by both the sender and recipient and computing this with a MAC generation algorithm like AES-CMAC or HMAC.

b)

A one-way hash function describes the computation of a variable input message into a fixed size hash value or message digest. The sender creates a message then generates a hash value of that message and sends both the message and the hash to the recipient. The recipient then compares the provided hash value to a hash value they generate upon receipt of the message to confirm the authenticity of the transmission. It is considered a one-way function because it is irreversible.

The difference between a MAC and a one-way hash function is that the hash function does not require a secret key as input.

TASK 3 – List the properties of a Strong Hash Function

1. The hash can be applied to a block or message of a variable size.
2. The hash value or digest produced is a preset / fixed length.
3. The computational effort to produce the hash value should be as lightweight and fast as possible.
4. The function is not reversible, e.g. it is impractical for an attacker to compute the message content of the hashed block from the hash itself.
5. It should be collision resistant where each hash value is unique and does not have a likelihood of being repeated for different message inputs.

TASK 4 – Differentiate between Public-Key Cryptosystems and Symmetric Encryption Algorithm

Public-Key Cryptosystems are asymmetric in that the system uses two different keys in the encryption and decryption steps known as the Public and Private Key Pair. One key is used for encryption and the other for decryption. This is different form a Symmetric Encryption Algorithm which uses the same key for both the encryption and decryption steps.

TASK 5 – In what way is the Diffe-Hellman key exchange algorithm insecure against a man-in-the-middle attack.

An unknown attacker, User C, in the middle of a communication chain between, User A and User B, can intercept the key exchange between the legitimate parties and substitute their own values without either of the authorised users being aware. In practice, when User A generates a key and transmits this to User B, User C then intercepts this key and substitutes their own, forwarding the new value to User B. Similarly, when User B responds to User A, User C intercepts this message and substitutes the legitimate value for another malicious one. Each intended sender and recipient believes the values to be legitimate even though they have been compromised. Now User C can read any messages exchanged between User A and User B.

TASK 6 – This is a problem that compares the security services that are provided by digital signatures (DS) and the message authentication code (MAC). The problem can be outlined as follows:

* There are three individuals, they are named, Alice, Charlie and Bob.
* Charlie is able to observe all the messages sent from Alice to Bob and vice versa.
* Charlie has no knowledge of the keys but the public one in case of DS.

For each of the scenario questions below, stat whether and how:

* i DS protects against the attack
* ii MAC protects against the attack

a) (Message integrity)   
Alice sends a message x = *“Transfer $1000 to Mark”* in the clear and also sends *auth (x)* to Bob. Charlie intercepts the message and replaces *“Mark”* with *“Charlie”*. Will Bob detect this? Explain why.

If using a Digital Signature which is follows the asymmetric authentication principles, then yes the message modification will be detected as the message thumbprint created by the hashing algorithm would not match what the one sent by Alice initially as the size of the message would be slightly different.

If the message was sent with a Message Authentication Code (MAC), similarly any change in the message content that is performed after the MAC is initially generated, a different value will be obtained when the receiver attempts to verify the MAC. When the MAC is originally generated it is based on the content of the original message and it is known that Charlie does not have the secret key for this exchange so his options are limited.

b) (Replay)   
Alice sends a message x = *“Transfer $1000 to Charlie”* in the clear and also sends *auth (x)* to Bob. Charlie observes the message and authorisation and sends them 100 times to Bob. Will Bob detect this? Explain why.

In the instance that the message is verified with a Digital Signature only then it is conceivable that the replay attack will not be detected as the content and the signature will pass the test each time.

If the message is protected with a Message Authentication Code then the replay would also likely not be detected as the code generated would be the same on every occasion.  
  
The only chance for this type of attack to be detected is if the repetition itself was cause for an alert, or if the message were to contain some kind of sequence number or other protection but as this is absent in the current scenario, then both the Digital Signature method alone and the Message Authentication Code method alone would not protect from the attack in this instance.

c) (Sender Authentication with cheating third party)   
Charlie claims that he sent some message *x* with a valid *auth(x)* to Bob, but Alice claims the same. Can Bob determine if either party is telling the truth? Explain why.

Yes, in both cases the authentic message can be determined as both the Digital Signature and Message Authentication Code can be validate as originating from Alice. Alice’s Digital Signature is created with her private key which Charlie cannot replicate and Charlie does not have the secret key used for the creation of the Message Authentication Code.  
d) (Authentication with Bob cheating)   
Bob claims that he received a message x with a valid signature auth(x) from Alice (eg. “Transfer $1000 from Alice to Bob”) but Alice claims she never sent it. Can Alice determine what may have occurred. Explain why.  
  
Yes Alice can determine what may have occurred in both cases but can only prove in one case that the message did not originate from her. In the Digital Signature scenario, Bob can’t produce a message with a valid signature so this protects against this type of attack as he does not have Alice’s private key and this can be proven.

In the case of a Message Authentication Code, both Bob and Alice have a common key so it is possible for Bob to produce a valid message which Alice may suspect – so yes she can determine what may have occurred, but ultimately unlike the Digital Signature scenario, she cannot prove that it did not originate from her. So the Message Authentication Code does not protect against this attack.