Lab 6 Solutions

SENG2250/6250

Part 1

Question 1

The use of multiple different factors in order to authenticate someone, these factors are defined as something the athenticatee is, has, or knows. An example would be, the user using a password (something the user knows) then scanning their fingerprint (something the user has).

Question 2

Three way authentication involves mutual authentication between two parties where the party that initiates the authentication acknowledges the other party's authentication by sending back $\{nonce_B, B\}_{SKA}$. Time synchronization is not required in this case since replay attacks are stopped by the final acknowledgment message as it contains the signed nonce of the other party. Since, A would have to know and acknowledge that it has just authenticated to B, then B may confirm that as true due to the use of signatures.

Question 3

In biometric-based authentication, identification mode refers to find a user's identity using the presented biometrics. A user does not need to claim its identity in this mode, instead, this mode may output 1 or more possible identities corresponding to the given biometrics. In the authentication mode, a user claims an identity and present the biometrics. The authentication server will check the validity of the provided information, then output Yes if a user is valid, otherwise, output No

Question 4

Access control restricts access to services based on the identity of the user, it requires the authentication of the user.

Question 5

Mandatory Access Control is the use of data classification schemes to give users limited access of that data. A form of MAC is the Access Control Matrix, where each user is given permissions for access to each of the resources, then each user and resource is given a security label. Those are then used to determine the true permission of the user to the object based on the model that is used.

Part 2

Question 6

A n-factor authentication is secure if and only if it secure when all of the possible $n-1$ factors are compromised.

In this case, the authentication is still secure if Bio and K is compromised as pwd is contained in an essentially salted hash. However, if K and pwd are compromised then entire authentication is compromised as the timestamp, TS, and the user's nonce, N_u, are public knowledge, and since K is compromised $E_K(Bio||N_u)$ may decrypted in order to break the entirety of the authentication.

Question 7

The **Bell-LaPadula Model** uses the rule read down, write up. The code is omitted here.

Question 8

a

HMAC is a message authentication code algorithm provided by hashing, MACs use symmetric keys, hence, they provide mutual authentication. So a HMAC would be good for user authentication.

b

The following is a python implementation,

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

import hashlib as hl

'''
Find HMACs and output in a terminal friendly format.

Author: Cody Lewis
Since: 2019-09-09
'''

def H(x):
    '''Hash the given message, x, and return the hex value.'''
    return hl.sha3_256(x).hexdigest()

def HMAC(k, m):
    '''
    Find the HMAC of the key, k, and the message, m, and return the hex value.
    '''
    k = int(bytes(k, "UTF-8").hex(), 16)
    m = bytes(m, "UTF-8").hex()
    opad = int("5c" * 32, 16)
    ipad = int("36" * 32, 16)
    return H(
        bytes.fromhex(
            hex(k ^ opad)[2:] + H(bytes.fromhex(hex(k ^ ipad)[2:])) + m
        )
    )

if __name__ == '__main__':
    KEY = input("Input a key: ")
    MESSAGE = input("Input a message: ")
    print(HMAC(KEY, MESSAGE))
```

Part 3

Question 9

a

Role Based Access Control is a form of Mandatory Access Control, however, RBAC determines authorizations for access to resources on a "role" basis. That is, a user would belong to a collection of roles and these roles state what resources are accessible. This is opposed to the Access Control Matrix models (Biba, Bell-LaPadula) which determine the access to resources on a user basis, in that the access levels have to be explicitly stated for each user to each resource.

b

Some advantages of RBAC:

- Easier to manage a few roles rather than many users
- Users may be given extra roles to allow for access to more resources
- Reduces memory usage if there are fewer roles than there are users

Some disadvantages of RBAC:

- Combinations of roles on users can become confusing and can potentially lead to giving a user more privilege than needed
- Specific rules for access control may lead to the need for the number of roles to be greater than or equal to the number of users