**Hsiang Lo**

**CS 370 Introduction to Security Week 7: Problem Set 7**

Instructor Name: Rakesh Bobba

# Introduction / Purpose

The purpose of this assignment is to help you gain a better understanding and insight into multi-factor aiuthentication, authentication protocols and biometrics covered in Week 7.

Before beginning make sure you have watched the lecture videos on the following and completed the associated practice quizzes.

* Multi-factor Authentication
* Biometric Authentication
* One-time Passwords
* Authentication Protocols

Chapter 3 till end of section 3.6 and Chapter 15 from Security Engineering: A Guide to Building Dependable Distributed Systems by Ross Anderson

# Instructions/Questions

Please answer the questions below.

## Multi-Factor Authentication?

Q1 [5 pts]: What is multi‐factor authentication? Give a real-world example of its use.

Multi-factor authentication is the usage of multiple elements/factors to prove identity. A real-world example is logging into Canvas. Not only do you need to know the password, which is something an entity knows, but you also need to enter a numbered/one-time password because it’s something an entity has, which is a phone for utilizing DUO authentication.

Q2 [5 pts]: Name four factors of authentication and provide an example for each one.

Four factors of authentication and their examples are as follow.

1. What entity knows, for example, password and private key
2. What entity has, for example, badge and smart key
3. What entity is, for example, fingerprints, retinal characteristics
4. What entity does, for example, voice pattern, handwriting
5. Where entity is, for example, in front of a particular terminal

Q3 [5 pts]: What is the difference between multi-factor authentication and mutual authentication (please look the latter up)?

Mutual authentication or two-way authentication takes place when both parties authenticates each other at the same time. This is different in that multi-factor is simply one party authenticating the other, but just with an extra layer, more protection.

## Biometrics

Q4 [5 pts]: What is a biometric? Give four examples of biometrics used for authentication.

Biometric is the measurement of biological or behavioral features that identify a person. It is under the category of what an entity is. Four examples of biometric used for authentication are as follows.

1. Fingerprints for accessing entrance to the gym.
2. Iris Pattern for government/high-level security logins.
3. Voice for google home activation
4. Faces for unlocking your phones

Q5 [4 pts]: What is the difference between static and dynamic biometric? Give two examples of each.

The difference between static and dynamic biometric differs in that static biometric is unchangeable. Dynamic biometrics on the other hand measures more of a pattern or behavioral pattern. Two examples of static biometrics – Fingerprints for unlocking your phone and using eye patterns in iris for nuclear code maybe? Dynamic examples include recording keystroke which is believed to be unique. Some characteristics measured are keystroke intervals, pressure, duration of stroke and where key is struck. Another example would be to use voices for speaker verification or recognition.

Q6 [4 pts]: What are advantages and disadvantages of using biometrics?

Advantage of biometrics means no more need to remember anything. Its intrinsic to the user. One disadvantage of using biometric is due to the fact that physical characteristics changes over time and some people may not be able to identify via specific characteristics.

## Authentication Protocols

Authentication protocol model

Q7 [6 pts]: Figure above shows a challenge-response protocol for static biometric authentication. KC is the shared key between the Host and the Client. B’ is user biometric captured by device.

BT’ is the biometric template computed from B’. D’ is device authenticator computed by

device. BT and D are biometric template and device authentication information at the Host.

Match(BT' BT) returns 'yes' if the user computed biometric matches with stored biometric

template at the host to within a certain pre-set threshold, and returns 'no' otherwise. Verify

(D', D) check the validity of the authenticator and returns 'yes' or 'no'. If all verifications

succeed at the host then the host returns 'yes' to client to indicate successful authentication.

1. [3 pts] What purpose does random number r serve? Put another way, if the protocol is modified to not include r what vulnerability does this introduce?

Random number r serves as a random challenge in order to provides authentication and defend against replay. In this case, if the protocol is modified to not include r, this could lead to vulnerabilities/problems such as session key reuse or replay attack.

1. [3 pts] Does message 3 from Client to Host need to be encrypted? Explain why. Specifically, won't integrity protection of this message using a keyed MAC be sufficient?

Yes, message 3 from Client to Host needs to be encrypted because when it is inside a hash function, even if someone sniff out this message, they still can’t see it and also because it’s a one-way hash, they can’t look back and reverse it. Passwords and information must be visible and provided in the clear in order for the system to authenticate, so hashing to protect the integrity is essential to rotect the message.

## One-time passwords

Q10 [6 pts] Consider the hash function h(i) = (i + 5) mod 7, and suppose it is used in an implementation of the S/Key protocol. Let the seed be value 0, and suppose that the first password the user returns after the initialization step is 4.

1. [4 pts] What password does the user return on the third login counting the first login password as 4.

Hash Function = H(i) = (i + 5) mod 7

1st Password = 4

2nd Password H(i) = (i + 5) mod 7 = 4,

Currently stored password is 6

3rd Password H(i) = (I + 5) mod 7 = 6

Currently stored password is 1

4th Password H(i) = (i + 5) mod 7 = 1

Currently stored password is 3

The third login password for the user is going to be 3!

1. [2 pts] On receiving this password, the server (chose one action below)
   1. **computes the hash of the returned password and admits the user if the hashed value is equal to the last correct password returned by that user**
   2. computes the hash of the last correct password returned by that user, and admits him if that value is equal to the password just returned
   3. uses the initial key to recompute the 3rd password by repeated hashing, and admits the user if the recomputed value is equal to the password the user returns

The correct answer is going to be A. Since the system compute the password the user gave and check it against previous password.

# Submission Details

Submit a PDF file with the questions and your corresponding answers

The assignment is worth 40 points. It is due Wednesday of Week 8 at Midnight.