**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.

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

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

## Biometrics

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

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

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

## 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?
2. [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?

## 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.
2. [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 valueis 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

# 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.