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.

- MFA is the use of two or more different methods of authentication in coordination to have more assurance that the person authenticating is who they claim to be. These two or more factors must address different aspects of how a person can authenticate – for example two passwords would not be considered effective MFA, as there is no increased guarantee that the person authenticating is who they claim to be. Contrast the two password example with proper MFA, where the user authenticates with, say, something they *know* (i.e. a password), *and* something they *have* (i.e. a hardware token). In this example, we are more sure that the person who is authenticating is who they claim to be as they showed us their hardware token and a password – two separate proofs of them being who they claim to be.
- A real world example could be that I want to enter into a CoLocation facility to administer company-critical system that are hosted therein. To confirm that I am indeed allowed to access, the system checks both a 10- digit pin (what you know, known only to those that are allowed access), and my biometrics (Fingerprints, Retinals, set when I was granted access to the CoLo facility). These together would constitute MFA.

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

- What you have – phone, hardware token
- What you are – finger prints, eye scan
- What you do – handwriting patterns, voice patterns

- What you know – password, pin

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

- Mutual Authentication refers to the process where two entities authenticate to each other – both are assured of the authenticity of the other. This is as opposed to multi factor authentication where a user provides multiple proofs of their identity to a server / target which does not authenticate to the user. That means that the user does not need / get to know that the server is who it claims it is as the only action that takes place is that the user proves their identity to the server, and not the other way around. For example, an SSH connection provides mutual authentication as the server must authenticate with the user, as well as the user authenticating to the server. Conversely, when I log into my bank (no SSL) I am not assured at all that I am logging in to my bank, as it does not authenticate to me, but the bank (if that is who is on the other end) is assured it is me, as I provide my password and my email second factor check.

Biometrics

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

- A biometric factor of authentication is something that is unique to the user who is authenticating. Otherwise put, biometrics are measurements of biological or behavioral traits specific to a person. This can include fingerprints, retinal scans, voice patterns recognititon and facial recognition.

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

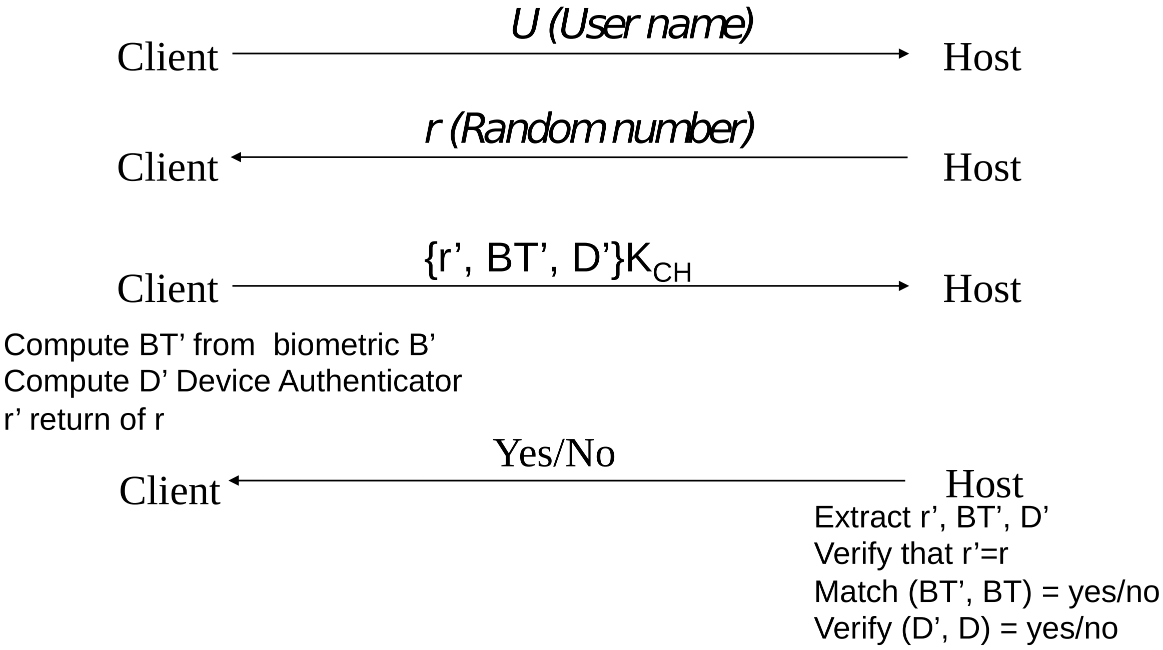
- Dynamic biometrics are biometrics that are with relation to things that the person authenticating does. For example, this might include gait (how a person walks), how someone types, speaks. Typically, these are calculated while the user inputs/ does them, and are most often ‘boiled down’ to statistical representations of what the user is doing. This is as opposed to static biometrics which are relatively constant over time, and do not require the user to be typing a password, walking or speaking (…) to get a reading. These include fingerprints, retinal scans and others.

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

- Advantages include the fact that biometrics are quite accurate, and when properly implemented (and when the proper biometric is chosen), these can be extremely hard to fake.
- Disadvantages are many, though, when talking about biometrics. Firstly, biometrics can be fooled by people seeking to bypass the biometrics. Also, people’s biometrics change over time, which can either lock someone out, or make it hard for the user to keep their biometrics up to date. Thirdly, some people lack some biometric characteristics as a result of their genetics. Specific technologies are required to read biometrics, and these

can be expensive. Also, biometrics are super important PII, and if they are not stored right, then they pose a risk of identity theft to the users. Lastly, where there is biometric authentication, there is the possibility of surveillance depending on how the information is shared and stored, and which actors want access. For example, if NSA were to have access to data from all fingerprint scanners on personal computers, they could establish a case against someone using the information and concrete proof that their fingerprint authentication succeeded at a certain time & IP address (as opposed to a password which *can* be easily faked).

Authentication Protocols



Q7 [6 pts]: Figure above shows a challenge-response protocol for static biometric authentication. K_C 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.

i. [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?
   - Without the challenge or nonce r, the replay vulnerability is introduced. This vulnerability would let an attacker replay message 3 at a later time to obtain a valid authentication for user "Client".

ii. [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?

- A keyed MAC would be great for protecting integrity, but message 3 contains the authentication data for that user, including their biometric template, which could be read (but not changed) if a MAC was used. This poses a security risk to the user Client.

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.

Server Hash Values$_{index}$: {~~0_0~~, 5_1, 3_2, 1_3, 6_4, 4_5, 2_6} | Server Keeps: 2

User Passwords in order: {~~2~~, 4, 6, 1, 3, 5}

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

- First login: User sends “4”, Second Login: User sends “6”, Third login: User Sends “1”/ Therefore, the user sends 1 on the third login.

ii. [2 pts] On receiving this password, the server (chose one action below)

a. **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**

b. 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

c. 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.