Andrew Plum

Mr. Alves-Foss

Cyb 110

9/4/21

Ch. 2 Homework

1) Identification is a claim about what someone or something is. Identification is the lowest level of knowing who is requesting access. Verification is a step beyond identification. During verification of an identity someone might show a form of ID, social security card, or birth certificate. However, this does not absolutely mean the claim to the identity is true. The person could be lying and have possession of these items to help him in claiming a false identity. Authentication improves on verification of identity in that it definitively establishes whether the claim of an identity is true. There are multiple methods of authentication. Some of the methods of authentication may include using a password, PIN, secret answer to a question, ATM card, cell phone, smart token, various kinds of biometrics (fingerprint scanner, iris scanner, etc.), etc. If more than one factor of authentication is used than it is called multifactor authentication. Multifactor authentication makes it more difficult for people to claim false identities.

3) The process in which the client authenticates to the server and the server authenticates to the client is called mutual authentication. Mutual authentication is an authentication mechanism in which both parties involved in a transaction authenticate each other. Mutual authentication makes sure that you are sending your transaction info to the actual server you want it to be sent to. When mutual authentication does not occur, you are at risk of impersonation attacks called man-in-the-middle attacks. In these attacks, the attacker impersonates both the client and the server to the eyes of the server and client respectively and can extract transaction information because of this if a transaction does occur. Implementing mutual authentication makes it significantly more difficult for the attacker to falsify to separate authentications. Mutual authentication can also incorporate multifactor authentication to make it even more difficult for the attacker.

6) If I am using an identity card as the basis for my authentication scheme, there are several steps I might add to the process in order to move to multifactor authentication. I might also ask for a password which would satisfy the “what you know” factor of authentication. If I wanted another “what you have” factor of authentication, I might also ask for the person to authenticate themselves through an app on their phone like the duo mobile app. If I added some sort of a biometric like a fingerprint scanner, this would satisfy the “what you are” factor of authentication. If I added signature recognition, this would satisfy the “what you do” factor of authentication. If I really wanted to be absolutely sure a person was who they claimed to be, you could implant a microchip in their body linked to their profile that would transmit their location which could be used as the “where you are” factor of authentication. This last method however would probably not be well accepted among people though. There are other things that could be done but implementing all these would satisfy all of the listed factors of authentication making this a multifactor authentication scheme.

7) Increasing the length of an all lowercase alphabet password from eight characters to ten characters would change the strength from 26^8 possible combinations to 26^10. Significant is a subjective term.

Now whether changing the possible combinations by a factor of 676 (26*26) is significant, this would actually be a greater increase in combinations than if you made the 8 character password incorporate uppercase and lower case characters. Changing the password to incorporate upper case and lower case characters would change the password from 26^8 possible combinations to 52^8 combinations. If you wanted to go even further to increase the strength of the password, you could incorporate numbers as well as special characters in your password. Despite all these changes to increase the strength of your password, of all the optional changes, increasing the length to your password would be one of the most efficient ways add strength to your password. I guess this would mean the change would be significant.

9) There are several factors of authentication I might use when implementing a multifactor authentication scheme for users who are logging onto workstations that are in a secure environment and are used by more than one person. I might use the “what you know” factor of authentication. This could include asking for a password or answering a secret question. I might use the “what you have” factor of authentication. This may include asking the person to authenticate themselves through an app on their phone like the duo mobile app. I possible could implement a fingerprint scanner biometric which would satisfy the “what you are” factor of authentication. The “what you do” factor of authentication would be a little bit difficult to implement here, but you could have it so that to access the system, you had to be authenticated through voice recognition. For the “where you are” factor of authentication, you could require that to access the system, you had to use devices associated to the system that are only in the secure work environment. These are just some of the things you could do to move to a multifactor authentication system.