CSCD 303 Essential Computer Security
Assignment 2
Fall 2017

Background

In class, we have been exploring the concepts of identify, authentication and authorization.
As we have observed, identity is difficult to preserve in the digital world. Authentication is imperfect since it is based on passwords and other mechanisms that can be stolen or fabricated. Authorization is based on the information provided so it is logical that mistakes will be made since the correctness of an authorization decision is based on imperfect mechanisms.

Task 1. - Explore Cogntive Biometrics

Cognitive biometrics is biometrics based on your ability to remember relevant information. This can be a form of lightweight two-factor authentication when visual queues in the form of pictures and passwords are used.

You will be using a free service called Passfaces.

1. Go to the website, www.passfaces.com/demo

2. A screen with a form to fill in pops up. Fill in the screen for First Time Users.

3. Click Start the Demo.

4. Go through the steps for using the faces shown through a series of screens.

5. Remember the faces shown to you. Go back to the beginning Passface screen.

6. Click Logon on the Returning users form on the right.

7. See if you can remember the faces to log on.

Answer the Following Questions
1.Is this an effective way to authenticate users?
2. Do you think it is good enough on its own or does it need to be combined with text based passwords?
3. Can this method be spoofed by a someone? In other words, can they figure out your passfaces and fake being you? Explain.
4. In two months from now, do you think you could recall the faces or would you forget?
5. Compare this to the pictures that are shown to you say on banking websites. Is this better, worse or the same?

Task 2 – Explore Single Sign On Methodology

We just touched on some existing technology for authenticating and authorizing access to resources in class. Touched on Kerberos, Radius and some other protocols. On-line providers have developed standards and technologies for single sign on so you do not have to log in to each site you visit. Most of

the time, you still have the option to create a password and log on to a given website. But, more and more the ubiquitous sites like Google and Facebook allow you to sign in with their credentials.

1. Explore OAuth. For this, you can google it. Hint, Google uses it for single sign on for their accounts. Explain. What is Oauth? How does it work ? Why would you want to use it instead of keeping private log-ins for your popular web services? Are there privacy concerns with using OAuth?

2. Explore OpenID. What is it? How does it work? How does it relate to Oauth? Is it the same type of service or different or in competition with it?

Answering the above questions should generate about a page of text. Not just one word answers and not a whole term paper of information. You can always improve your explanations by including pictures or diagrams. Of course you can cut and paste these … just be able to explain them.

Deliverables

1. Turn this one in hard copy, please. Put CSCD303 – Assignment 2 at the top and Your Name too.
2. Bring it to class on the due date.

Thank you.