**DBA-210 Database Administration**

**Final Exam 2017FA**

Immigration cards holding both passport number and measures of the user’s hand; fingerprints taken as a legal requirement for a driver license, but not stored anywhere on the license; automatic facial recognition systems searching for known card cheats in a casino; season tickets to an amusement park linked to the shape of the purchaser’s fingers; home incarceration programs supervised by automatic voice recognition systems; and confidential delivery of health care through iris recognition: these systems seem completely different in terms of purpose, procedures, and technologies, but each uses “biometric authentication” in some way.

This week, I want you to explore some of the technologies and applications that make up the field of “biometric authentication” – what unites them and what differentiates them from each other. “Biometric Technologies” are automated methods of verifying or recognizing the identity of a living person based on physiological or behavioral characteristics.

For your final exam, I want you to research and learn some things about biometric authentication techniques. Keeping in mind that the data from these will have to be stored somewhere and that, as a DBA, it will be your job to help determine when, where, and how of biometrics for your company.

Please answer the first three questions about biometric authentication. Use thorough research, give me the URL or other identifying information where you find your sources (does not have to be in a particular format) and answer each question fully and completely as if your boss was asking for this information.

In addition, it will fall to the DBA’s shoulders frequently to either devise or participate in the making of a disaster recovery plan. Should disaster occur like fire, flood, tornado, or complete system failure, then what will happen and how will you get your data center back online in the most efficient fashion and lose the least amount of data? The last two questions deal with disaster recovery. Please answer as fully and completely as you can.

1. List four biometric authentication techniques, briefly explain how each one works including a list of advantages and disadvantages. (20)

* Face recognition – this analyzes features that are common to everyone’s face such as distance between eyes, size of nose, position of cheekbones, jawline, etc. These measurements are combined into a single code the uniquely identifies each person. The benefits of this technique are that it works even when the subject is unaware that they are being scanned. Unfortunately, as some iPhone users have found recently, the face recognition can be unlocked while a user is sleeping, giving access to anyone else. With the newest iPhone X, this problem may no longer be an issue.

<https://www.theregister.co.uk/2017/09/13/apple_iphonex_facial_recognition/>

* Fingerprint identification – this technique compairs the patterns of ridges and furrows on the fingertips with a database of prints on file. Fingerprint identification works well because no two fingerprints are the same, giving everyone a unique identifier. However, some more elementary fingerprint scanners are optical and can be unlocked with a spoof that replicated the look of the fingerprint. Spoofs can be made out of things like silicone, gelatin, or glue.

<http://wkar.org/post/msu-team-works-improve-fingerprint-security#stream/0>

* Retina scan -

2. List and explain 3-4 fundamental barriers that may limit the growth of biometric authentication. (20)

3. List and explain 3-4 best practices and things to consider for implementing biometrics authentication systems. (20)

4. Disaster Recovery Plan – Write a short well constructed paragraph explaining what it it and who needs it. (20)

5. Find two companies that provide disaster recovery services for small to medium size businesses. Briefly discuss each of them, including comparing and contrasting them as appropriate. (20)