**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 – this technique scans the pattern of blood vessels at the back of the eye. The advantage of this is that there is no known way to replicate a retina. On the negative side, retina scans do not work for those who have lost their sight. As shown in this article, that can cause very dire consequences for those people.

<https://thewire.in/201934/unable-verify-fingerprints-iris-aadhaar-denies-leprosy-patients-basic-services/>

* Voice analysis – this technique is the same as face recognition where it can be done without the users’ knowledge. An advantage to this technique is that it is not possible to fool the analyzer by imitating a voice, however, you can fake a voice such as using a taped recording.

<http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16>

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

Some barriers against the growth of biometric authentication are social acceptance, cost, and accessibility. Consumers are often worried about their privacy and the potential misues of data which can deter people from accepting the use of biometrics. While the security that biometrics offers is definetly worth the investment, the cost for building a biometrics database, implementing the technology, and educating users may be too high. Going back to the previously linked article involving the woman who was denied her pension because she couldn’t pass the biometric scans, accessibility may be an issue for some users.

<https://www.americanbanker.com/opinion/overcoming-the-barriers-to-biometrics>

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

There are a few things to consider before implementing biometric authentication systems. The first is that some biometrics, like fingerprints, can be lifted and used by someone else. Secondly, biometrics are hard to reset since your password is now a physical feature of your body. Third, it is possible for hackers to use copies of a user’s biometric characteristics collected by the system to produce fake biometics that allow them to login.

<https://www.globalsign.com/en/blog/biometric-authentication-considerations/>

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

A disaster recover plan is a process implemented to have a SQL server running and to overcome data loss in the event of a disaster. For this plan to be effective, it must be executed before a disaster happens. The first step of creating and executing a disaster recovery plan involves taking stock of inventory, identifying priorities, implementing the SQL disaster recovery plan, and integrating that into the companies DR plan. Once you have an idea of what you will need for the DR plan, you can begin designing and developing the plan. Once you deploy the DR plan, the DBA will do periodic reviews, testing, and refinement of the recoverability.

Anyone using a SQL server database can benefit from a disaster recovery plan. As the DBA responsible for the database, your job could be on the line if you are not able to recover your company’s data after a disaster. Many companies cannot function without or afford to lose even a small amount of data. DR plans are more than just backing up data, it is practicing the recovery and being prepared.

<https://www.sqlshack.com/sql-server-disaster-recovery/>

<http://www.itprotoday.com/microsoft-sql-server/smart-dbas-guide-sql-server-disaster-recovery-part-1>

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)

Plan B Disaster Recovery and Zetta Disaster Recovery are providers of disaster recovery solutions for SQL servers. Arcserve provides a free trial, however Plan B does not. Both provide instant recovery and protection for both physical and virtual servers on public and private clouds. With Plan B, you have access to specialist engineers who can provide tech support and help. Plan B also tests the replica system every day for flaws. They also offer custom solution designs.

Zetta Disaster Recovery may be the better option for a less technical user with it’s simple and effect ‘push-button’ recovery. This product also looks to be the more cost-effective for smaller businesses that may not be able to afford a more pricey disaster recovery service. Zetta also offers experts to assist in the initial setup and testing of the service. Their engineers are available to help during failback to make sure the transition after a disaster is as smooth as possible. Zetta uses cloud-based disaster recovery requiring no on-premise device.

<http://www.techradar.com/news/top-5-best-disaster-recovery-services>

<https://www.zetta.net/zetta-disaster-recovery>

<https://www.planb.co.uk/services/>