JSAL Database Redundancy and Security Design

1. Introduction

In this document JSAL presents the database redundancy and security design for the eVote Sparrow and Raven. It explains the different options available for redundancy, and the team's approach on how to implement the security for the system.

2. Redundancy

Due to the nature of electronic voting, it is essential that all the data be stored on a system that provides the following: availability, fault-tolerance, and performance throughout the whole election process. In the case of a natural or human-made disaster, the data must not be lost or corrupted. This can be resolved by utilizing Redundant Array of Independent Disks (RAID). There are several levels of RAID in the market; JSAL presents some of the advantages and disadvantages of the levels to be considered [1]:

- RAID 1
    - Advantages:
        - 100% redundancy of data means no rebuild is necessary in case of a disk failure, just a copy to the replacement disk.
        - Under certain circumstances, it can sustain multiple simultaneous drive failures.
        - Simplest RAID storage subsystem design.
    - Disadvantages:
        - Highest disk overhead of all RAID types (100%) – inefficient.

- RAID 5
    - Advantages:
        - Highest Read data transaction rate.
        - Medium Write data transaction rate.
        - High efficiency.

    - Disadvantages:
        - Disk failure has a medium impact on throughput.
        - Most complex controller design.
        - Difficult to rebuild in the event of a disk failure (as compared to RAID level 1).
- RAID 6
    - Advantages:
        - Protects against multiple bad block failures while non-degraded.
        - Protects against a single bad block failure while operating in a degraded mode.
        - Perfect solution for mission critical applications.
    - Disadvantages:
        - More complex controller design.
        - Requires N+2 drives to implement because of dual parity scheme.
- RAID 10
    - Advantages:
        - RAID 10 has the same fault tolerance as RAID level 1.
        - Under certain circumstances, RAID 10 array can sustain multiple simultaneous drive failures.
        - Excellent solution for sites that would have otherwise gone with RAID 1 but need some additional performance boost.
    - Disadvantages:
        - Very expensive, high overhead.
        - Very limited scalability at a very high inherent cost.

Finally the last, but not the least, factor to consider when deciding which RAID level to use is monetary cost. This will depend on the budget of the aspiring client.

3. Security

Since the eVote system handles sensitive information (i.e. passwords, votes), certain measures were taken to encrypt the data that will be stored in the database. JSAL decided to use the AES encryption and decryption functions already integrated with MySQL. They are considered to be the most cryptographically secure encryption functions currently available in MySQL [2]. Here is the syntax of the functions:

- AES_ENCRYPT(*str*, *key_str*) where *str* represents the data to be encrypted and *key_str* represents the key, or password, to use for encryption.
- AES_DECRYPT(*crypt_str*, *key_str*) where *crypt_str* represents the encrypted data and *key_str* represents the key, or password, to use for decryption.

Figure 1 illustrates how the security will work in the eVote system. Each administrator will have their corresponding password. With this password the administrator will be able to log in into the system. The password will be stored in the database, using itself as the key. Therefore, when an administrator logs in, their password will be encrypted using the password as the key and the result will be compared to their corresponding encrypted password stored in the database.

Once in the system, there will be 104 master keys where each master key will correspond to a precinct [3]. These will be stored in the database already encrypted. These master keys will be used to encrypt/decrypt the votes stored in the database. In order for this to work, JSAL implemented an intermediate key that will permit the administrator to decrypt the encrypted master key. These keys will be temporarily stored in the main application, once a session has started these keys will be requested to a central voting center and then stored in the application. This was implemented taken into consideration, the administrator. JSAL did not want the administrator to be aware of an intermediate key, nor add the burden of handling a second password.

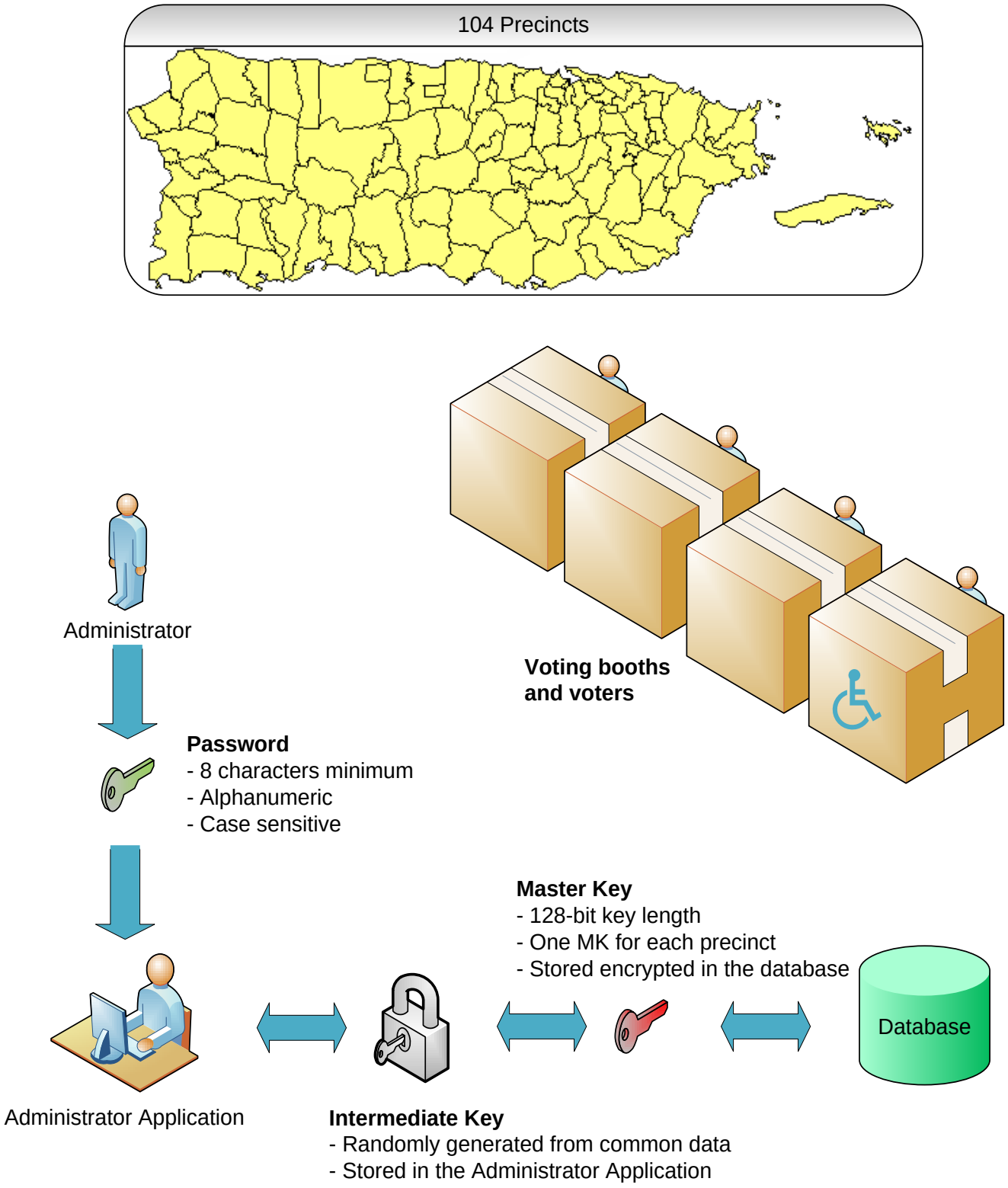

Figure 1: eVote security implementation

4. Glossary

- **Fault-tolerance**: also known as fail-safe, enables a system to continue operation, possibly at a reduced level, rather than failing completely, when some part of the system fails [4].
- **Overhead**: any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to be utilized or expended to enable a particular goal [5].

5. References

[1] "RAID Tutorial & Benchmarking Tools." AC&NC. 6 Dec. 2008 . [Online].Available: http://www.acnc.com/04_00.html

[2] "MySQL 5.0 Reference Manual: Encryption and Compression Functions." MySQL: Developer Zone. 6 Dec. 2008.[Online].Available: http://dev.mysql.com/doc/refman/5.0/en/encryption-functions.html

[3] "Elecciones Generales 2000: Mapas Interactivos - Precintos." Comisión Estatal de Elecciones de Puerto Rico. 19 Dec. 2000. 6 Dec. 2008. [Online].Available: http://www.ceepur.org/elecciones2000/escrutinio/mapas/precintos.html

[4] "Fault-tolerant design." Wikipedia. 1 Sep. 2008. 6 Dec. 2008. [Online].Available: http://en.wikipedia.org/wiki/Fault_tolerance

[5] "Computational overhead." Wikipedia. 13 Nov. 2008. 6 Dec. 2008. [Online].Available: http://en.wikipedia.org/wiki/Computational_overhead

Silberschatz, Abraham, Henry F. Korth, and S. Sudarshan. Database System Concepts (5th Edition). Boston: Mcgraw-Hill College, 2005.

Stallings, William. Cryptography and Network Security (4th Edition). Alexandria, VA: Prentice Hall, 2005.