Database Security Assessment

Chimene Tchokoko Diboma

School or Institution Name (University at Place or Town, State)

**Database Security Assessment**

**Overview for Vendors:**

The military hospital is a leading hospital providing healthcare services to not only military personnel but to the general public as well. Hospital has a main administrative department that is responsible for all of the management tasks related to hospital management. Administration department keeps the records of doctors and related staff. The accounts department of the hospital manages the payroll system and all financial activities (Bertino, 2015). There are different sections related to the specific treatments of designated diseases such as cancer ward is only reserved for the treatment of cancer patients and related research. Coordination between the departments is managed by the administration department. The hospital currently has 700 employees including the doctors, nurses, paramedics, and administrative staff.

Hospital is using manual record maintenance methods to keep a track record of all management activities such as patient visits, appointments, and billing, etc. The hospital requires an automated hospital database management system. The required database management system must be able to handle massive workloads with a high quality of service. The central database will have records related to all departments. The database management system will be responsible for maintenance, usage, and operations of the central database. Critical information such as Patient medical history along with personal details, diagnostics, billing details, employees’ personal details, payroll history, and management will be stored in the database. As all the departments will have coordinated services, a relational database will always serve the purpose of keeping the records maintained (Dhillon, Torkzadeh, & Chang, 2018). It will enable all the departments to have up to date information records of a particular patient. Depending on the sensitivity of the information being stored in the database system, the hospital required the competing vendors to ensure compliance with the highest standards of cybersecurity. Despite the relational nature of the database, there must be appropriate levels of data segregation. So, the information related to the finance department cannot be accessed or manipulated by other departments beyond authorized limits.

Different departments and staff members will use the system as per their requirements. Nurses will use the system to view and update patient health records. The receptionist will use the system to arrange appointments of the patients with doctors. Ward boys will use the system to manage the patient visits to the hospital such as preparation of the discharge slips. Administrative staff will use the system to monitor activities of all the departments, attendance of the doctors, and other members of the hospital staff. The accounts department will use the system to establish payroll, salary management, and billing information of the patients. Overall the system will be the central management system of the hospital and will provide the stated functionalities.

**The context for the Work:**

The hospital requires appropriate segregation between the data elements stored in the database management system. As the system will provide users with an intuitive web-based user interface, the vendors must demonstrate the ability of their system that there are no critical security loopholes in the system. Web-based applications use error handling techniques to provide users with useful information and troubleshooting steps. However, such error handling if not implemented appropriately can be used by the attackers to infiltrate into the database and compromise sensitive information records (Nazareth & Choi, 2015). The vulnerability in database management systems due to the improper handling of errors is known as the information leakage. Information leakage can happen when the database management systems fail to limit the amount of information provided with the error. Competing vendors must demonstrate the ability of the proposed system in the proposal that the web application is capable of sanitizing the messages generated by the sequential query language or database management system.

As the hospital requires a web-based interface to provide access to the central database to multiple departments, the system must be sufficiently protected against cross-site scripting attacks. In a cross-site scripting attack also known as the XSS attack, an attacker can inject the malicious code in a trusted webpage. The script is executed when the user loads the page embedded with the malicious script. Cross-site scripting attacks can allow the attackers to compromise the entire network of the organizations. XSS attacks may soon replace the injection attacks on SQL database systems (Boulares, Adi, & Logrippo, 2015). Therefore, the proposed system must be protected against XSS attacks. The proposed system must ensure that there will be no broken authentication vulnerabilities. As the data segregation requirements will be coupled with the authentication system, it must be secure enough to block man in the middle attacks. Strong authentication mechanisms must be used to overcome the authentication flaws of the relational database systems. Access control will also be an important assurance required from the participating vendors. The system must provide essential access controls to limit the information exposure as per the defines user rules in the system.

**Vendor Security Standards:**

It is a critical requirement of the hospital from all participating vendors to focus on the confidentiality, integrity, availability, and non-repudiation of the data stored in the system. To confirm with the security standards of the proposed system a security and processes checklist will be available for testing purpose. Proposed solutions will be tested against the common criteria that are a global set of rules and regulations to test the security performance of information management systems. Common criteria rules are mostly used to test the security products proposed for the implementation of critical government departments. However, depending on the sensitivity of information processed using the proposed system, it must comply with the common criteria (Schinagl, Paans, & Schoon, 2016). Vendors submitting proposals for the hospital must provide certificates confirming their solutions with both the key components of common criteria such as protection profiles and evaluation assurance levels. The vendor must provide the certification that the proposed solutions are configured for the highest standard profile of data protection.

The required protection profile is that the database must be encrypted using sophisticated encryption algorithms employing AES-256 keys. If the data is encrypted, then the attackers will not be able to compromise sensitive information of the patients even if they are able to break logical defenses such as firewalls and access control mechanisms. An encryption system is as secure as the keys associated with the encryption. Therefore, the management system of the database will ensure that none of the departments will have access to the complete key of encryption. Instead of having access to the full key of encryption, all the departments must have different chunks of the key to ensure non-repudiation of data (White, Fisch, & Pooch, 2017). The second component of the common criteria provides evaluation assurance levels. The scale used for evaluation assurance levels is from 0 to 7 with 7 being the highest level of evaluation. However, a product rated at 7 does not guarantee that it will have maximum security and performance standards implemented. It only provides information that the product has undergone a maximum number of security and performance evaluation tests.

The vendors must provide the information in the proposal about the security target of the product. Security target of the product provides information about the threats the product tested against. Vendor’s self-assessment results must also be attached to the proposal. If the product is tested by a third party testing agency, then the authorized certificate must be attached to the proposal. Even if the products tested against the vendor's self-assessment criteria, they will be tested for disaster recovery operations. The required evaluation level assurance is that the system must be able to recover itself from disaster state with a minimum time limit of one hour. Any system taking a long time for disaster recovery will not be suitable as per the service level requirement of the hospital. High level of continuity in operation is required from the proposed system.

**Defense Models:**

All the databases and systems will be connected using the internal network of the hospital. The internal network will contain ethernet connections and wireless connections for different systems. Enclave computing environment will be established in the hospital to protect against cyber-attacks. Each section of the hospital buildings will use a boundary defense mechanism for the networks. Each section will use a separate switch that will be configured with access control lists to block the outside access. A central firewall will protect the network against hackers. However, departmental firewalls will protect the wireless connections of the employee devices (McDougall & Woodruff, 2016). As the firewall defense is not enough against all of the hacking attempts, end devices will be equipped with host-based intrusion detection systems. A firewall only considers the attacks originating from outside of the network. The host-based intrusion detection system will halt the attacks originating from within the network.

Network equipment installed within a department will be considered as the boundary of enclave environment. Access control lists implemented in each department will help in the protection of data segregation level. As the general medical staff will not be able to access the information related to the finance department due to the blocking rules defined in the access control lists. Along with the access control lists, the officials working in the same department will have different levels of permissions such as read and write access to the databases. For example, the receptionist will have the read access to the information of the doctors but will not have the write permission to edit any relevant information. Each network will be separated from the other using a department level firewall. Such firewall configuration will allow the networks to be protected against hacking attacks. Even if the network of one department is compromised by the hackers infiltrating the network rest of the departments will remain separated from the malicious traffic. The hackers will not be able to compromise the entire network (Roslan, Hamid, & Shamala, 2018).

The defense model proposed must be able to defend the critical infrastructure against distributed denial of service attacks. In a distributed denial of service attacks, hackers use a large network of computing devices infected with the malware. Hackers cause congestion on the network links by generating fake service requests to the server. Legitimate traffic is blocked from accessing the service. As the hospital require high availability of the service, the vendors must ensure that the denial of service attacks will not be able to compromise the network.

Access control methods will be implemented as per the policies of the Department of Defense. The internal security policies of the hospital will also comply with the policies defined by the department of defense. It is crucial while designing the internal cybersecurity policies for different departments to understand the usability requirements of the system. There exists a tradeoff between the security and usability of the system. A most secure system will be the one disconnected from everything. If that system is then buried in a block of concrete that will be the most secure system on earth. As it will not be possible for anyone to access that system. However, the same system will be the most useless system on earth as well. Therefore, designing internal security policies of the hospital ill be all about finding the best balance between security and usability of the system.

**Requirement Statement for System Structure:**

The proposed system will be used by patients as well. The user interface and the web-based portal is required to be customized for each user group. The doctors must be provided with all access to alter the patient information such as diagnostic, medications, and comment on laboratory test results. Doctors must not be provided with permission to alter the details about the appointments. Appointments with the doctors will be altered by the administrative staff only. The restrictions must be enforced to ensure the continuity of operations (Chapple, Stewart, & Gibson, 2018). If multiple users’ groups will be provided with similar rights, then there will be operational difficulties. The administrative staff of the hospital will be provided with the consolidated access to the databases as they have to monitor the functionalities of different departments. Receptionists and paramedics will be allowed to alter or update the records of appointments of patients with the doctors.

All of the departments will have strict regulations regarding data protection. None of the users must have permission to transfer data using external media devices. Such data exfiltration restrictions are inevitable to avoid the misuse of medical information. Cyber-criminals target employees of organizations using social engineering techniques. An employee may connect an infected external media device containing the malicious code to the system. Once, the malicious code is executed on the machine it will be very difficult to contain the damages caused by the malicious actor. The restriction may affect the usability of the system in rare cases. To prevent such usage restrictions the higher management must be provided with a feature to enable data transfer using external media devices for a short period of time.

**Operating System Security Components:**

Operating systems are the core components of any computing device. An operating system is responsible for the management of the hardware resources and it provides applications with a working environment as well. The operating system of the installed devices must use virtualization for processes so that processes executed on the machine by one application cannot alter the processes executed by a different application. Applications requiring administrative rights on a machine can bypass such restrictions. To avoid exceptions to this scenario, effective security policies must be implemented by the vendor to create a secure ecosystem for applications (Laracy & Marlowe, 2018). Operating systems installed on end-user devices must be pre-configured to update all of the installed applications regularly. It is mandatory for the operational continuity of the hospital as most of the cyber-attacks happen due to the security holes present in outdated applications. Software level attacks can be prevented using strong security policies at the operating system level.

It is required by the competing vendors to ensure that all of the supplied devices have trusted platform modules installed and correctly configured to be used with mission-critical applications. Trusted platform module also known as the TPM, is a hardware chip that is used to store authentication credentials, user certificates, and cryptographic keys. TPM provides a tamper-proof environment for applications to store and manage the credentials. The space provided by the TPM for credential storage cannot be compromised by software attacks. TPM chips must be present in all the network devices as the encryption keys will be stored in them. End-user devices will have TPM chips pre-installed on their main circuit boards (Jacobs, 2015). Such TPM chips are used by the operating systems to store sensitive information. The TPM chips can verify the hardware platform as well. For example, at the boot time, the contents of the TPM will be checked for integrity. In case of any tampering signs, the user will be restricted from accessing mission-critical applications on the device.

Trusted platform modules can protect encryption keys and other user authentication certificates. However, TPM chips cannot control the applications running on the machine. Meaning that a malicious application running on the machine may alter the contents of a TPM. Therefore. There must be security processes implemented at each level such as network and operating system (Wu, Chen, Yang, & Du, 2019). All the logical measures such as operating system hardening tools, patch management applications, trusted platform modules, and firmware create a trusted computing environment. Each component of the infrastructure will be validated and checked for integrity by the system before allowing access to critical functions of the installed system including the storage databases.

**Requirements for Multiple Independent Levels of Security:**

Multiple independent security levels can be used by the vendors to control the authentication and access to the data. These multiple security levels are based on the Biba or Bell-LaPadula models of security. As per these models the user groups of one consolidated access. Users of one group cannot alter or access the files of users with higher rights. Similarly, the users of one rights group cannot alter or access the files of groups with lower user rights. Similar access restriction model is known as the Chinese wall model that restricts the access to file objects based on the conflict of interests. The models are explained in the orange book of the DoD (McMillin & Roth, 2017). However, such models if not implemented with care can provide backdoor access to the attackers. The requirement of the hospital is to provide a system that is capable of insecure handling of files using the Biba model. Files must be tied to encryption algorithms and must not be transferred to any external medium. The hospital does not require the access mechanisms to be online as all the departments will access the central database locally.

**Test Plan requirements:**

Vendors will use the Biba model to restrict access to files for different user groups. The Biba model works on the principle that the user of the one group cannot access or alter the files of higher as well as lower rights user groups. Such implementation of access restrictions can be bypassed by the cross-site scripting attacks. The proposed solution will be tested for cross-site scripting attack for the insecure handling of data. A script will be injected into the critical web interface of a database and level of damage or access rights violation will be recorded. If the attack is recorded to be successful, then security measures will be implemented by the vendors to patch the vulnerability as soon as possible (Cai et al., 2018). SQL injection using the user input method will also be tested for any visible security flaws. All of the discovered flaws will be patched by hardening the security policies regarding user input methods.

Authentication and access control systems are central to the overall security posture of the system. Any broken authentication or access system can lead to the overall compromise of the system. It would not be beneficial to invest in secondary systems for the protection of an already installed system of authentication and access control. In case of any broken system. Certificate-based authentication system will be implemented for all the users regardless of their rights. Secure access system will be enforced by using digital signatures-based file handling mechanism.

**References:**

Bertino, E. (2015). Big data-security and privacy. *2015 IEEE International Congress on Big Data*, 757–761. IEEE.

Boulares, S., Adi, K., & Logrippo, L. (2015). Information flow-based security levels assessment for access control systems. *International Conference on E-Technologies*, 105–121. Springer.

Cai, F., Zhu, N., He, J., Mu, P., Li, W., & Yu, Y. (2018). Survey of access control models and technologies for cloud computing. *Cluster Computing*, 1–12.

Chapple, M., Stewart, J. M., & Gibson, D. (2018). *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*. John Wiley & Sons.

Dhillon, G., Torkzadeh, G., & Chang, J. (2018). Strategic Planning for IS Security: Designing Objectives. *International Conference on Design Science Research in Information Systems and Technology*, 285–299. Springer.

Jacobs, S. (2015). *Engineering information security: The application of systems engineering concepts to achieve information assurance*. John Wiley & Sons.

Laracy, J. R., & Marlowe, T. (2018). *Systems Theory and Information Security: Foundations for a New Educational Approach*.

McDougall, A., & Woodruff, J. (2016). Physical security management. In *Handbook of SCADA/Control Systems Security* (pp. 286–307). CRC Press.

McMillin, B., & Roth, T. (2017). Cyber-physical security and privacy in the electric smart grid. *Synthesis Lectures on Information Security, Privacy & Trust*, *9*(2), 1–64.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), 123–134.

Roslan, S. N., Hamid, I. R. A., & Shamala, P. (2018). E-Store Management Using Bell-LaPadula Access Control Security Model. *JOIV: International Journal on Informatics Visualization*, *2*(3–2), 194–198.

Schinagl, S., Paans, R., & Schoon, K. (2016). The revival of ancient information security models, insight in risks and selection of measures. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 4041–4050. IEEE.

White, G. B., Fisch, E. A., & Pooch, U. W. (2017). *Computer system and network security*. CRC press.

Wu, Z., Chen, X., Yang, Z., & Du, X. (2019). Reducing Security Risks of Suspicious Data and Codes through a Novel Dynamic Defense Model. *IEEE Transactions on Information Forensics and Security*.