ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 6, No.18 , November 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Developing an Allocation Framework for Information Security Systems

Abdel Nasser H. Zaied[1], Walid I. Khedr[2] and Shimaa S. Mohamed[3]

[1] Dean, Faculty of Computer and Informatics, Zagazig University, Zagazig, Egypt
nasserhr@gmail.com

[2] Information Technology department, Faculty of Computer and Informatics, Zagazig University, Zagazig, Egypt
wkhedr@zu.edu.eg

[3] Decision Support department, Faculty of Computer and Informatics, Zagazig University, Zagazig, Egypt
Shimaa_said1100@yahoo.com

Abstract

Databases hold a critical concentration of sensitive information and become available on the internet to facilitate access, and as a result, databases are vulnerable and become the target of hackers. Today the security of database system become one of the most urgent tasks in database research, so to protect database system from attacking and compromised through authorized users who abuse or misuse data and unauthorized users who made unprivileged access. In this paper most of database vulnerabilities and threats which may face database system are reviewed and allocated proposed security techniques to protect database system from these threats to reduce risk of attacking database system.

Keywords: *Database Threats, Database Threats components, Security Techniques, Allocation Techniques, SQL Injection.*

1. Introduction

Data is most important and valuable asset in today's world as it helps organizations as well as individuals to extract information and use it to make various decisions and it is used in day-to-day life. Data are generally stored in database so that retrieving and maintaining it becomes easy, efficient and manageable. At a very general level, a database can be defined as a persistent collection of related data, where data are facts that have an implicit meaning. Typically, a database is built to store logically interrelated data representing some aspects of the real world, which must be collected, processed, and made accessible to a given user population. The database is constructed according to a data model which defines the way in which data and interrelationships between them can be represented [1]. As database have huge amount of sensitive information it is important to know challenges which face database system to protect it from attacking.

2. Database Threats and Vulnerabilities

With the increase in access to data and information stored in databases, the frequency of attacks against those databases has also increased. A database threat refers to an object, person or other entity that represents a risk of loss or corruption of sensitive data and sensitive information to an asset also database threats may be caused because of vulnerabilities in database system [2]. Attacks on database can also be classified into passive and active attacks [3]:

- **Passive Attack**: attacker only observes data present in the database. Passive attack can be done in following three ways (Static leakage, Linkage leakage, and Dynamic leakage).
- **Active Attacks**: actual database values are modified. These are more problematic than passive attacks because they can mislead a user, for example a user getting wrong information in result of a query. There are some ways of performing such kind of attack Spoofing, Splicing, and Replay.

Attacks on database can be used to disclose information, to sidestep authentication mechanisms, to alter the database, and to execute arbitrary code, in certain instances, on the database server itself. Attackers can be categorized into internal and external. External person is an intruder who gains access to a computer system and tries to infiltrates a database server to steal or tamper with data information. Internal, insider is an authorized user in database system that belongs to the group of trusted users and tries to get information that he is unauthorized to access, or administrator is a person who has privileges in administering a computer system, but abuses his rights and his power in order to extract valuable information; no database security can be guaranteed [4]. According to Ponemon Institute [5] in his study, the average total cost per data breach increased 15 percent to $3.5 million, and average cost per lost or stolen record increased more than 9 percent from $136 in 2013 to $145 in this year's study.

2.1 Database Threats and Vulnerabilities Components

In the period from 1999 to 2015, many researchers studied types of database threats and vulnerabilities; they classified them into 22 threats as follows:

2.1.1 SQL Injection Attack (SQLIA)

Imperva defined SQL injection attack as insertion (or "injection") of unauthorized SQL database statements into a vulnerable SQL data channel. SQLIA is considered anyone who can send untrusted data to the system. Typically, targeted data channels included stored procedures and Web application input parameters [6 & 7]. OWASP concluded that using SQL injection, attackers may gain unlimited access to a whole database and to the potentially sensitive information these databases contain [8].

The sources of SQL Injection can be one of the following [2]**:**

a. Injection through user input; malicious strings in web forms in web application.
b. Injection through cookies; modified cookie fields contain attack strings.
c. Injection through server variables; headers are be manipulated to contain attack strings.
d. Second-order injection; Trojan horse input seems fine until is used in a certain situation. Attacks don't occur when it first reaches the database, but when is used later on.

2.1.2 Weak Authentication

Amichai studied weak authentication as allowing the attackers to steal the identity of authorized database. An attacker may define any number of strategies to obtain credential. Weak authentication schemes allow attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials [9].
Approaches that an attacker may employ to obtain credentials as [9 & 10]:

- **Brute Force** – This approach attacker repeatedly enters all possible username/password combinations until he finds one that works.
- **Social Engineering** – This approach the attacker takes advantage the natural human tendency to trust in order to convince others to provide their login credentials.
- **Direct Credential Theft** – Here attacker may steal login credentials by copying post-it notes, password files, etc., Center's (ADC) ongoing research into proprietary database communication protocols and vulnerabilities.

2.1.3 Unmanaged Sensitive Data (Unauthorized Copies of Sensitive Data)

Many companies struggle to maintain an accurate inventory of their databases and the critical data objects contained within them. Forgotten databases may contain sensitive information, and new databases can emerge – e.g., in application testing environments – without visibility to the security team. Sensitive data in these databases will be exposed to threats if the required controls and permissions are not implemented [6 & 7]. Also, many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes [8].

2.1.4 Storage Media Exposure (Backup Data Exposure)

Backup storage media is often completely unprotected from attack (Unencrypted data on backup tapes and disk). As a result, numerous security breaches have involved the theft of database backup disks and tapes. Furthermore, failure to audit and monitor the activities of administrators who have low-level access to sensitive information can put your data at risk [9].

2.1.5 Web application attacks

Web application attacks through poorly configured websites, applications and databases. Today, the focus of exploitation has shifted from the operating system to the Web browser and multimedia applications. Web applications being used as the major platform for the flow of sensitive information there is increasing security concerns for the organizations as well as for the individuals. Due to transaction of high sensitive corporate information through the web and increase in online traffic multifold the security issue [11]. Web applications are vulnerable to a variety of well publicized attacks, such as cross-site scripting (XSS) and Cross-Site Request Forgery (CSRF) [12].

2.1.6 Buffer Overflow Attacks

A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer or unauthorized user causing the application to perform an action the application was not intended to perform. The overall goal of a buffer overflow attack is to subvert the function of a privileged program so that the attacker can take control of that program [13 & 14].

2.1.7 Advanced Persistent Threat (APT)

An advanced persistent threat (APT) is a kind of network attack in which an unauthorized person gains access to a network and stays there hidden for a long period of time. APT usually targets organizations and or nations for business or political motives. APT processes require high degree of covertness over a long period of time. As the name implies, APT consists of three major components/processes: advanced, persistent, and threat. The advanced process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The persistent process suggests that an external command and control is continuously monitoring and extracting data off a specific target. The threat process indicates human involvement in orchestrating the attack [15 & 16].

2.1.8 Covert Channel

Steven defined covert channel as means of communicating on a computer system, where both the sender and receiver collude to leak information, over a channel not intended for the communication taking place, in violation of a mandatory access control security policy and consider it as a computer security attack which can be used to weaken the system's security policy [17].

2.1.9 Unpatched DBMS

In database vulnerabilities are remain changing that can be exploited by unauthorized user, database suppliers release patches to ensure sensitive information in databases is protected from attackers. Once these patches are released they should be patched immediately. If left unpatched, hackers can reverse engineer the patch, or can often find information online on how to exploit the unpatched vulnerabilities, leaving a DBMS even more vulnerable that before the patch was released [18]. Attackers release unpatched vulnerabilities which can occur at any layer of a system which have sensitive information.

2.1.10 Redundant DBMS Features Enabled

There are many unnecessary features which are enabled by default in DBMS. And these unnecessary features should be turned off. If these unnecessary features are not change off so by this it can be dangerous attack on database. Attackers will only have more to use against you [18].

2.1.11 Broken Configuration Management (Misconfiguration)

Unwanted features are enabled in DBMS due wrong configuration. Incorrect or Unnecessary Implementation of Security at any Layer of a System Security misconfiguration can occur at any layer of a system. The user will provide unauthorized access or knowledge of a system for attackers [8].

2.1.12 Inference (Statistical Inference)

This is a database system technique which used to attack databases where malicious users gather sensitive information from complex databases at a high level. It is performed by analyzing number of different data sources in order to illegally get knowledge about a database. In basic terms, inference is a data mining technique used to predict and find information hidden from normal users. An inference presents a security breach if more highly classified information can be inferred from less classified information [19 & 20].
There are two inference vulnerabilities in database [3 & 20]:

Data Association: It occurs when two values have been taken together. And those are classified at a higher level than the classification of either value individually.

Data Aggregation: it occurs when a set of information is classified at a higher level than the individual level of data.

2.1.13 Social Engineering

Social engineering (known as non-technical or human-based attack) describes a method of launching attacks against information and information systems and targeting the existing vulnerabilities of both people and technology; as a result it is considered as the biggest security threat faced by both organization and individuals today. The types of information these attackers are seeking can vary, trying to ploy you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them control over your system [21].

2.1.14 Malware

Malware defined as software designed to attack and damage, disable, or disrupt computers, computer systems, or networks this mean that website malware can imagine, this makes website malware particularly insidious and dangerous. Malware includes Viruses, Worms, Spyware, Trojans, Bots, and other malicious programs. The reasons that make website vulnerabilities to malware, website owners continue to increase their website's popularity. Also increased interactivity on websites can introduce exploits that open the door to malware [22].

2.1.15 Database Rootkits

Rootkit is code or program or procedure run on a system by an intruder, or changes made to a system's internal state in order to retain control of key system resources without detection by user or administrator. Rootkits are often categorized as a variant of malware but differ in several important respects. The fundamental difference is scale of target – they're narrowly targeted, with a specific mission and capture and optionally modify specific data over a period of time without detection "Rootkits are used as a means of carrying out espionage". In order to install a rootkit, an attacker will require the ability to execute code on the target system. Furthermore, the attacker will need to run this code with administrative privilege, or exploit vulnerability in the operating system [23].

2.1.16 Excessive Privilege Abuse

When database users are provided with the access rights that allow them to perform other tasks not included in their job (users have privileges exceed their job requirement), these privileges may be abused purposely or accidentally, harmful intent can be discovered through such tasks thus leading to misuse of such privileges. For example, in a university administrator whose job requires only the ability to change student contact information may take advantage of excessive database update privileges to change marks [10 & 24].

2.1.17 Legitimate Privilege Abuse

Users will abuse legitimate database privileges for unauthorized purposes. When the authorized user misuses the authorized privilege for illegitimate purpose, this is the mean legitimate privilege abuse. For example a hypothetical rogue healthcare worker has privileges to view individual patient records via a custom Web application. The structure of the Web application normally limits users to view an individual patient's healthcare history – multiple records can't be viewed simultaneously and electronic copies are not allowed. However, the rogue worker can circumvent these limitations by connecting to the database using an alternative client such as MS-Excel and MS-SQL. Using MS-Excel, MS-SQL Server or Oracle and his legitimate login credentials, the worker may retrieve and save all patient records [6].

2.1.18 Privilege Elevation

Privilege Elevation Attackers may take advantage of database software vulnerabilities to discover flow of flaws which is taken advantage of by attackers and may result in the change of privileges such as converting access privileges from those of an ordinary user to those of an administrator. Vulnerabilities may be found in, built-in functions, stored procedures, protocols implementations, and even SQL statements. For example, a software developer at a financial institution might take advantage of a vulnerable function to gain the database administrative privilege. With administrative privilege, the rogue developer may turn off audit mechanisms, transfer funds, create bogus accounts, misinterpretation of certain sensitive analytical information, etc. [9 & 24].

2.1.19 Database Platform Vulnerabilities

Vulnerabilities in operating systems vulnerabilities and additional services installed on a database server could lead to leakage easily. Vulnerabilities in the previous operating systems such as Widows 98, Windows 2000, UNIX, etc. may lead to unauthorized access, data loss from a database, data corruption or service denial conditions. For example, the blaster worm created denial of service conditions from vulnerabilities which found in Windows 2000 [2].

2.1.20 Database Communication Protocol Vulnerabilities

Maximum numbers of security vulnerabilities are being identified in the database communication protocols of all database vendors. Four out of seven security fixes in the two most recent IBM DB2 FixPacks address protocol vulnerabilities1. Similarly, 11 out of 23 database vulnerabilities fixed in the most recent Oracle quarterly patch relate to protocols. Fake of activity targeting these vulnerabilities can range from unauthorized data access, to data corruption, to denial of service. For example, the SQL Slammer2 worm, took advantage of a flaw in the Microsoft SQL Server protocol to force denial of service and to carry out code on targeted database server [9 & 10].

2.1.21 Weak Database Audit Trail

Weak Database Audit Trial defined as automated recording of database transactions involving all sensitive data should be part of any database deployment and the database security considerations. Failure and absence (weak or non-existent) to collect detailed audit records of database activity may cause instability in operations and represents a serious organizational risk on many levels; such as regulatory risk, prevention, detection and recovery, this mean that audit policies that rely on built-in database mechanisms suffer a number of weaknesses that limit or preclude deployment [10 & 24].

2.1.22 Denial of Service (DOS) Attack

Denial of service (DOS) conditions could be created by many techniques which are related to the other mentioned vulnerabilities in database such as database platform vulnerabilities to crash database server. For example, attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, attempts to prevent particular individuals from accessing a service and attempts to disrupt service to a specific system. This attack is very serious attack [6 & 7].

3. Experimental Analysis

In this paper are made experimental analysis on previous 22 threats and vulnerabilities, these analysis was based on some features of database threats such as Attack type, Source of threats, Exploitability, Impact, and Users as shown in table (1). Attack type feature refer to Active or Passive attack all threats are active attack but inference threats, and when this attack happen which attack on database system (Database Server, Web Server, Browser, Network Infrastructure, and Operating System Attack). Source of threats feature refer to where this attack may happen such as Internal mean that this attack happened inside the system (Intra-organization-LAN Network), External mean that this attack happened outside the system (Extra-organization-WAN Network), and Internal - External mean that this threat may happen inside and outside system. Exploitability feature refers to ability users to hack system such as Easy, Average, Difficult, and Very Difficult. Easy means that freely available exploit code, exploit SQL Injection, Platform vulnerabilities, database vulnerabilities and there are easy to install malicious programs which download itself to users' computers without their knowledge such as malware. Average mean that attackers need administrative privilege, analyze number of different data sources in order to illegally get knowledge about a database, or need to know identity of authorized users before attack. Difficult mean privileged users who can access sensitive data. Very Difficult mean that attackers need to access network as privileged user and stay unknown for long time and target privileged users as in Advanced Persistent Threat (APT) threat. Impact feature refer to degree effect threat on system such as Severe and Moderate. Severe mean that the attackers can do anything the victim to obtain privileges of authorized users and reputation of organization could be harmed, Lack of accountability, Denial of service, Lead to complete host takeover. In this feature all data could be stolen, modified, or deleted and reputation of organization could be harmed also business impact of public exposure of the vulnerabilities, all accounts or some of them can be attacked as in SQL Injection, Weak Authentication, Unmanaged Sensitive Data, Backup Data Exposure, Legitimate Privilege Abuse, Database Platform Vulnerabilities, and Database Communications Protocol Vulnerabilities. Also may subvert the function of a privileged program, corrupt data, crash the program, and execute malicious code as in Buffer Overflow Attack. Attacker's goal in this feature may steal data rather than cause damage to the network or organization. APT attacks target organizations in sectors with high-sensitive information, for instance national defense, manufacturing and the financial industry. Malware attack cut corners with insufficient input validation on user input, inadequate logging mechanisms, and using fail-open error handling or failing to close a database connection. Penetrate organizations and steal sensitive data and including identity theft and financial ruin. Damage, disable, or disrupt computers, computer systems, or networks and loss your reputation, loss of customer trust and goodwill, downtime due to blacklisting and non-compliance issues violations. Rootkits may also modify the database object itself and change the execution path and switch off alerts triggered by Intrusion Prevention Systems (IPS) and modify a running operating system kernel in order to hide an attacker's presence. Not discovered after compromising a system. Excessive Privilege Abuse and Privilege Elevation in these attacks any "minor" breach becomes a major incident, gain DBA access (full control of the database), complete operating system control, and turn off audit mechanisms. DOS Attack cause data corruption, network flooding, resource consumption and resource server overload (memory, CPU, etc.), disrupt connections between two machines, prevent particular individuals from accessing a service and disrupt service to a specific system, crash database server (database is unavailable), paralyzing the entire operations of an organization or part of it. Moderate Features means that attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, and redirect user's browser and impact to your reputation as in Web Application Attack. Also because of weak the system's security policies lead to leak sensitive information and financial losses and damage also reputation of organization is affected as in Cover Channel and Social Engineering Attack. Also all of data could be stolen or modified slowly over time, the system could be completely compromised without you knowing it, traffic, or full database take over, and recovery costs could be expensive as in Unpatched DBMS, Redundant DBMS Features Enabled, and Broken Configuration Management (Misconfiguration). All high classified data could be stolen, modified, or deleted, Could your reputation be harmed as in Inference Attack. Also Weak Database Audit Trial limits or precludes deployment such as Lack of User

Accountability, Performance Degradation, Separation of Duties, Limited Granularity and Proprietary.

Table 1: Database threats Features

Threats	Attack Type	Threats Source	Exploit	Impact
SQL Injection	Database Server Attack	Internal - External	Easy	Severe
Weak Authentication	Database Server Attack	Internal - External	Average	Severe
Unmanaged Sensitive Data	Database Server Attack	Internal	Difficult	Severe
Back up Data Exposure	Database Server Attack	Internal	Difficult	Severe
Web Application Attacks	Web Server Attack	External	Average	Moderate
Buffer Overflow Attack	Web Server Attack	External	Easy	Severe
Advanced Persistent Threat	Network Infrastructure Attack	Internal - External	Very Difficult	Severe
Covert Channel	Computer Security Attack	External	Average	Moderate
Unpatched DBMS	Database Server Attack	Internal	Easy	Moderate
Redundant DBMS Features Enabled	Database Server Attack	Internal	Easy	Moderate
Broken Configuration Management	Database Server Attack	Internal	Easy	Moderate
Inference	Database Server Attack	Internal - External	Average	Moderate
Social Engineering	Web Browser Attack	External	Difficult	Moderate
Malware	Web Server and Browser Attack	Internal - External	Easy	Severe
Database Rootkits	Web Server and Database Server Attack	Internal - External	Average	Severe
Excessive Privilege Abuse	Database Server Attack	Internal	Easy	Severe
Legitimate Privilege Abuse	Database Server Attack	Internal	Easy	Severe
Privilege Elevation	Database Server Attack	Internal	Difficult	Severe
Database Platform Vulnerabilities	Operating System Attack	Internal	Easy	Severe
Database Communication Protocol Vulnerabilities	Database Server Attack	Internal - External	Difficult	Severe
Weak Database Audit Trial	Database Server Attack	Internal	Difficult	Moderate
Denial of Service Attack	Database Server, Web Server and Network Infrastructure Attack	Internal - External	Easy	Severe

4. Proposed Security Techniques

The database attackers will gain money by selling sensitive information, which includes credit card numbers, Social Security Numbers, criminal records and important organization information etc. So, the need to insure the integrity of the data and secure the data from unintended access is emerged. To secure a database environment, many database security techniques are developed [2]. Database security depends on a set of systems, processes, roles, and procedures that can protect the database from unintended activities. Unintended activities can be categorized as authenticated misuse, malicious attacks or inadvertent mistakes made by authorized individuals or processes. The importance of database security will continue to grow as more data is shared, retained, transmitted and archived electronically [25]. After previous discussion, to protect database from hackers there are security techniques must implemented to avoid system from attackers.

4.1 Techniques to fight with SALIA

The detection approaches for SQLIA can be categorized broadly into pre-generated and post-generated approaches. Post-generated approaches are generally useful while analyzing dynamic SQL which is generated by web application such as Positive tainting and Syntax aware evaluation, Context Sensitive String Evaluation, Parse tree

evaluation based on grammar and DUD [Debasish, Utpal and D.K. Bhattacharya] approach. Pre-generated approaches are generally used during the testing phase of the web application such as Pixy and Program Query Language. Also Application layer intrusion detection approach which breaks data into buckets as done in network intrusion detection system. Relative frequencies of those buckets are used to compare with the historical data to decide about the intrusion, or Use prepared statements and parameterized queries to fight with SQLIA [3 & 10].

4.2 Digital Certificate and PKI

Digital certificate are electronic files that are used to identify people and resources over networks such as the Internet. Digital certificates also enable secure, confidential communication between two parties using encryption. Public Key Infrastructure (PKI) provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the three principal security functions (integrity, authentication and nonrepudiation). A PKI is a combination of hardware and software products, policies and procedures. It provides the basic security required for secure communications so that users who do not know each other or are widely distributed, can communicate securely through a chain of trust. Digital certificates are a vital component in the PKI infrastructure as they act as 'digital passports' by binding the user's digital signature to their public key [26].

4.3 Encryption

Encryption / It prevents exposure of sensitive information even if the database server is compromised so that when a database is compromised by an intruder, data remains protected even when a database is successfully attacked or stolen. Furthermore, database encryption can be employed to maintain the data integrity, ensuring that even a little modification made on the data can be detected. Database encryption technology meets the data confidentiality requirements and has become an indispensable aspect of enterprise database security [27].

4.4 Http Proxy Server Firewall

The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall [28].

4.5 Access Control Mechanism

Access Control Mechanism is a technique to maintain data confidentiality. When someone tries to access data object, Access Control Mechanism checks the rights of the user against set of authorizations. They are generally specified by security administrator or security officer. Authorizations are given as per the security policy of the organization. Along with Access Control Mechanism, A strong Authentication mechanism is also required to authenticate the valid user of a database system. After that access control will help defining different access permissions on different data objects of a database [29].

4.6 Enforcing Buffer Size Limitation

An effective way to prevent an overflow is to strictly enforce the buffer's size limitation. Simply stated, never allow more data to be placed into a buffer than it is designed to hold. Stack validation, a critical part of an overflow attack is modifying the return address pushed onto the stack by the caller. Once the called procedure returns using the altered return address, control is passed to the attacker's code and the attack succeeds. If the called procedure could detect the stack tampering, the application could terminate itself before executing the attacker's code. By pushing a static value onto the stack and validating it before returning, a called procedure can avoid passing control to malicious code. These static values are often called *static canaries* or *canary values*, and are used in products such as StackGuard and the Immunix Secured OS. When the buffer is overflowed to change the return address, the canary value is overwritten because it is located between the buffer and the return address. By checking the value of the canary before returning from the procedure, it is possible to thwart the attack by terminating the process before the attacker's code is executed [30].

4.7 Data Scanning and Analyzing Tools

Security managers have turned to scanning and analysis tools to identify a wide variety of potential problems on their networks. While host-oriented patch tools such as Update EXPERT from St. Bernard Software and HFNetChkPro from Shavlik Technologies focus on the myriad patches needed to keep Windows servers up to date, network vulnerability analyzers look for more than just missing patches. These tools can search for misconfigured application servers, such as Web servers; and network components, such as switches and routers. They look for out-of-date applications, especially those

with known problems. And they often search for applications that are enabled by default--but perhaps shouldn't be, such as RPC services on UNIX or the UDP ECHO program on Windows NT/2000. They often look for "information leakage" from systems through DNS and other avenues, including SNMP and Windows registry [31].

4.8 Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Bases Access Control (RBAC)

Access control mechanisms of current DBMSs are based on discretionary policies governing the accesses of a subject to data based on the subject's identity and authorization rules. Mandatory access control (MAC) policies regulate accesses to data by subjects on the basis of predefined classifications of subjects and objects in the system. Objects are the passive entities storing information, such as relations, tuples in a relation, or elements of a tuple. Subjects are active entities performing data accesses. RBAC models represent arguably the most important recent innovation in access control models. RBAC models are based on the notion of role. A role represents a specific function within an organization and can be seen as a set of actions or responsibilities associated with this function. Under an RBAC model, all authorizations are granted to the role associated with that activity, rather than being granted directly to users. Users are then made members of roles, thereby acquiring the roles' authorizations. User access to objects is mediated by roles; each user is authorized to play certain roles and, on the basis of the roles, he can perform accesses to the objects [29].

4.9 Anti-Phishing Software

Over the past few years we have seen an increase in "semantic attacks" — computer security attacks that exploit human vulnerabilities rather than software vulnerabilities. Phishing is a type of semantic attack in which victims are sent emails that deceive them into providing account numbers, passwords, or other personal information to an attacker. Typical phishing emails falsely claim to be from a reputable business where victims might have an account. Victims are directed to a spoofed web site where they enter information such as credit card numbers or Social Security Numbers. Billions of dollars are lost each year due to unsuspecting users entering personal information into fraudulent web sites. To respond to this threat, software vendors and companies with a vested interest in preventing phishing attacks have released a variety of "antiphishing tools." For example, eBay offers a free tool that can positively identify the eBay site, and Google offers a free tool aimed at identifying any fraudulent site. As of September 2006, the free software download site **Download.com**, listed 84 anti-phishing tools [32].

4.10 Anti-Malware Tools

Anti-malware refers to software tools and programs designed to identify and prevent malicious software, or malware, from infecting computer systems or electronic devices. Anti-malware tools can also include malware removal capabilities, and the term anti-malware can range from code integrated with other software programs or in the operating system itself to third-party tools that scan for and remove a wide variety of malware variants. Also anti-malware software is commonly thought of as software tools for desktops and laptops, but anti-malware tools also abound for servers, workstations and mobile devices like smartphones and tablets [33].

4.11 Rootkit Detector and Remover tools

Sophos Virus Removal Tool will scan your computer and let you safely and reliably detect and remove any rootkit that might have hidden itself on your system. As part of its complete protection of endpoint computers, Sophos End user Protection has an integrated detection functionality that removes and prevents them being installed onto your desktops, laptops and servers [34].

4.12 Intrusion Detection System

Intrusion detection is a security technology that attempts to identify either individual who is trying to break into system and misuse information without authorization and\or those who have legitimate access to the resource but are taking undue advantage of their rights. The job of Intrusion Detection System (IDS) is to dynamically monitor the events occurring in a system and alert when any suspicious activity occurs so that defensive action can be taken to prevent or minimize damage. In general, the main goal of IDS is to detect malicious transactions before they are being committed and then dropping and rolling them back. Intrusion detection systems serve three essential security functions: they **monitor**, **detect** and **respond** to unauthorized activity [35].

4.13 File Integrity Monitoring

File Integrity Monitoring (FIM) is an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often

involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. The Verisys File Integrity Monitoring system provides a simple solution to your integrity monitoring requirements, giving you confidence that the integrity of your data has not been compromised [36].

4.14 Database Activity Monitoring

Database Activity Monitoring (DAM) is a database security technology for monitoring and analyzing database activity that operates independently of the database management system (DBMS) and does not rely on any form of native (DBMS-resident) auditing or native logs such as trace or transaction logs. DAM provides privileged user and application access monitoring that is independent of native database logging and audit functions. It can function as a compensating control for privileged user separation-of-duties issues by monitoring administrator activity. DAM is a powerful solution that independently monitors and audits all database activity across multiple database platforms. It provides an easy-to-use audit trail policy for all sensitive tables and columns, administrative access, and a "before and after" view of all changes. Some DAM solutions include full monitoring of applications and other sources of database calls [37].

4.15. Database Firewall

A firewall forms a barrier through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction. A firewall may be designed to operate as a filter at the level of IP packets, or may operate at a higher protocol layer. Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet. A firewall may act as a packet filter. It can operate as a positive filter, allowing passing only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria. Depending on the type of firewall, it may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets [28].

4.16 SSL and WTLS

Secure Sockets Layer (SSL) technology is a security protocol that is today's de-facto standard for securing communications and transactions across the Internet. SSL has been implemented in all major browsers and Web servers, and as such, plays a major role in today's e-commerce and e-business activities on the Web [38]. The Wireless Application Protocol (WAP) is a standard to provide mobile users of wireless phones and other wireless terminals access to telephony and information services, including the Internet and the Web. WAP security is primarily provided by the Wireless Transport Layer Security (WTLS), which provides security services between the mobile device and the WAP gateway to the Internet [28].

5. Allocation Proposed Security Techniques

Proposed resource allocation approach first: determined which security techniques to assign to each database threat based on experimental analysis, this analysis based on features of database threats from perspective of hackers. In this research are made experimental analysis on 22 previous threats and vulnerabilities, this analysis was based on some features/characteristics of database threats such as how attacker made unauthorized access on database system at each threat, Attack type, Location of threats, Exploitability, Impact, Users, and Scope. Attack type feature refer to Active or Passive attack, all threats are active attack but inference threat is only passive attack, and when this attack happen which attack in database system (Database Server, Web Server, Browser, Network Infrastructure, and Operating System Attack). Location of threats feature refer to where this attack may happen such as Internal mean that this attack happened inside the system (Intra-organization- Local Area Network (LAN)) and External mean that this attack happened outside the system (Extra-organization-WAN Network). Exploitability feature refers to ability users to hack system such as Easy, Average, Difficult, and Very Difficult. Impact feature refer to degree effect threat on system such as Severe and Moderate, in this research not focused on low threats impact as these threats not important. Users feature refer to who can made unauthorized access on system, authorized means that attacker privileged but made misuse or abuse data and unauthorized means that attacker unprivileged access system as privileged user. Scope feature refer to impact threat on security services such as confidentiality, access control, integrity, and availability. All these features of threats are shown in previous experimental study.

This allocation approach **second**: decide where objects (Security techniques) are allocated free for database threats based on location of threat and impact of threat on system. In this research threats classified into internal threats and external threats based on source of threats. In this research database threats classified into internal database threats and external database threats, Table (2) determines internal

threats which happen inside organization, and proposed security techniques which must implemented on data inside system such as Use prepared statements and parameterized queries (SQLIA), Anti-malware tools, Rootkit Detector and Remover tools, Data and Memory Encryption, Data scanning and analyzing tools, and Access Control or on internal communication of LAN Network such as all other proposed security techniques in table (2), also these threats arranged according to impact threats.

Table 2: Internal Database Threats

Threats	Impact	Proposed Security Techniques
SQL Injection	Severe	Use prepared statements and parameterized queries, and use Pre-generated approaches, Post generated approaches, Application layer intrusion detection approach, and SAFELI approach
Weak Authentication	Severe	Use Certificates and PKI
Unmanaged Sensitive Data	Severe	Data Encryption Access control
Back up Data Exposure	Severe	Data Encryption
Advanced Persistent Threat	Severe	Deploy Memory/Data Injection Prevention Technologies Memory and Network Encryption
Malware	Severe	Anti-malware tools
Database Rootkits	Severe	Rootkit Detector and Remover tools
Excessive Privilege Abuse	Severe	Deploying IDS to detect Insider Attacks
Legitimate Privilege Abuse	Severe	Deploying IDS to detect Insider Attacks
Privilege Elevation	Severe	File integrity monitoring
Database Platform Vulnerabilities	Severe	Database Activity Monitoring Database Firewalls
Database Communications Protocol Vulnerabilities	Severe	Use SSL & WTSL
Unpatched DBMS	Moderate	Data scanning and analyzing tools
Redundant DBMS Features Enabled	Moderate	Data scanning and analyzing tools
Broken Configuration Management	Moderate	Data scanning and analyzing tools
Inference	Moderate	MAC, DAC, and RBAC
Weak Database Audit Trial	Moderate	Audit duties should ideally be separate from both database administrators and the database server platform to ensure strong separation of duties policies

Table (3) determines external threats which happen outside organization, and proposed security techniques which must implemented to protect system, these techniques implemented on user's system such as Use prepared statements and parameterized queries (SQLIA), Anti-malware tools, Rootkit Detector and Remover tools, and Use anti-phishing software or implemented on external communication of internet such as all other techniques, also these threats arranged according to impact threats.

Table 3: External Database Threats

Threats	Impact	Proposed Security Techniques
SQL Injection	Severe	Use prepared statements and parameterized queries, and use Pre-generated approaches, Post generated approaches, Application layer intrusion detection approach, and SAFELI approach
Weak Authentication	Severe	Use Certificates and PKI
Buffer Overflow Attack	Severe	Strictly enforce the buffer's size limitation
Advanced Persistent Threat (APT)	Severe	Deploy Memory/Data Injection Prevention Technologies Memory and Network Encryption
Malware	Severe	Anti-malware tools
Database Rootkits	Severe	Rootkit Detector and Remover tools
Database Communications Protocol Vulnerabilities	Severe	Use SSL & WTSL
Web Application Attacks	Moderate	Use http proxy servers firewalls
Covert Channel	Moderate	Use resource monitoring techniques
Inference	Moderate	MAC, DAC, and RBAC
Social Engineering	Moderate	Use anti-phishing software

From two previous tables, there are threats which occurred inside and outside organization such as SQL Injection, Weak Authentication, Advanced Persistent Threat, Inference, Malware, Database Rootkits, and Database Communications Protocol Vulnerabilities. Also Denial of Service attack doesn't have supported techniques as it is difficult to prevent DOS attack but can discover the reason of this attack and solve the problem.

6. Conclusions

As databases hold a critical concentration of sensitive information, and as a result, databases are vulnerable, so database systems become the favorite target for hackers. In this paper vulnerabilities and threats which may face database system are survived and from previous analysis concluded that these threats impact on database system for all in database server, web server, browser, network infrastructure, and operating system, these mean that all part of database system become attacked from hackers. So today, enhancing the security of database is becoming one of the most urgent tasks in database research and industry to protect database system and to prevent compromised database. Also Audit duties should ideally be separate from both database administrators and the database server platform to ensure strong separation of duties policies (Regulatory Problem). Also must use resource monitoring which obtaining information concerning the utilization of one or more system resources and it is used to monitor the change in computer resources that caused by malware execution**.**

References

[1] Sabrina. D. C. V, Pierangela. S, Sushil. J, 1999, "Database Security", "European Community within the FASTER Project in the Fifth (EC) Framework Programme under contract IST-1999-11791", pp. 1-21

[2] Nedhal A. Al and Dana. Al, 2013, "Database Security Threats: A Survey Study", "International Conference on Computer Science and Information Technology (CSIT)", pp.60-64

[3] Saurabh. K and Siddhaling. U, 2012, "Review of Attacks on Databases and Database Security Techniques", "International Journal of Emerging Technology and Advanced Engineering", pp.253-263

[4] Erez. S, Ronen. V, Ehud. G and Yuval. E, 2014," Implementing a database encryption solution, design and implementation issues", "computers & security", pp. 33 – 50

[5] Ponemon Institute, 2014, "2014 Cost of Data Breach Study: Global Analysis / Research Report", "IBM - Ponemon Institute LLC", pp.1-28

[6] Imperva's Application Defense Center, 2013, "Top Ten Database Security Threats" "Data Security for the Data Center", pp.1-11

[7] Imperva's Application Defense Center, 2014, "Top Ten Database Security Threats" "Data Security for the Data Center", pp.1-9

[8] OWASP, 2013, "The Ten Most Critical Web Application Security Risks", "the Open Web Application Security Project - OWASP", pp. 1-22

[9] Amichai. Sh, 2006, "Top Ten Database Security Threats", "CTO Imperva, Inc.", pp.1-14

[10] Shivnandan. S and Rakesh. K. R, 2014, "A Review Report on Security Threats on Database", "(IJCSIT) International Journal of Computer Science and Information Technologies, pp. 3215 – 3219

[11] Abdul Razzaq, Ali. H, Nasir. H and Farooq. A, 2009, "Multi-Layered Defense against Web Application Attacks", "Sixth International Conference on Information Technology: New Generations", pp.492-497

[12] Andrew. B, Dan. B and Palash. N, 2007, "Exposing Private Information by Timing Web Applications", "the International World Wide Web Conference Committee (IW3C2)", pp.1-8

[13] Crispin. C, Perry. W, Calton. P, Steve. B and Jonathan. W, 1999, " Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade", "IEEE, and Proceedings of DARPA Information Survivability Conference and Expo (DISCEX)", pp.1-11

[14] James. C. F, Vitaly. O, Nish. B and Niels. H, 2005, " Buffer Overflow Attacks: Detect, Exploit, Prevent ", "Syngress, Inc.", pp.1-521

[15] Damballa, Inc., 2010, "Advanced Persistent Threats (APTs)", available at "https://www.damballa.com/advanced-persistent-threats-a-brief-description/" 9/1/2015

[16] Sam. M, 2014, "Advanced Persistent Threat – APT", available at "https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT" 9/1/2015

[17] Steven. J. M, 2007, "Technical Report: Covert channel vulnerabilities in anonymity systems", "UCAM-CL-TR-706 / ISSN 1476-2986", pp.1-140

[18] Mark. T, 2012, "Top 10 Database Vulnerabilities and Misconfigurations", "APPLICATION SECURITY, Inc.", available at "http://www.sifma.org/uploadedfiles/societies/sifma_internal_auditors_society/top10-database-vulnerabilities-and-misconfigurations.pdf" 1/1/2014

[19] Salvador. M, 2000, " Inference Attacks to Statistical Databases: Data Suppression, Concealing Controls and Other Security Trends", Aleph Zero online magazine, number 23", pp.1-12

[20] Emil. B, 2009, "DATABASE SECURITY - ATTACKS AND CONTROL METHODS", "JAQM: JOURNAL OF APPLIED QUANTITATIVE METHODS / Software Analysis", pp.499-454

[21] Lech. J. J and Lingyan.R. F, 2010, "Social Engineering-Based Attacks: Model and New Zealand Perspective", "IEEE, International Muliconference on Computer Science and Information Technology", pp.847-853

[22] Jim. R, 2012, "The Ongoing Malware Threat: How Malware Infects Websites and Harms Businesses — and

What You Can Do to Stop It", "Symantec Corporation - VeriSign, Inc, pp.1-11
[23] John. H, 2006, "Rootkit threats", "NGS – New Generation Software", pp.18-19
[24] Iqra. B, Farooque. A, and Abdul Wahab. M, 2012, "Database Security and Encryption: A Survey Study ","International Journal of Computer Applications (0975 – 888)", pp.28-34
[25] Kevin. K, 2006, "Cryptography in the Database: The last line of Defense", "USA, Symantec Corporation", pp.4-11
[26] Ray. H, 2001, "PKI and Digital Certification Infrastructure", "9th IEEE International Conference on Networks (ICON.01)", pp. 234 – 239
[27] Gang. Ch, Ke. Ch, and Jinxiang. D, 2006, "A Database Encryption Scheme for Enhanced Security and Easy Sharing", "10th International Conference on Computer Supported Cooperative Work in Design", pp. 1-6
[28] William. S, (2011), "Cryptography and Network Security Principles and Practices, Fifth Edition", "publishing as Prentice Hall", pp. 1-900
[29] Elisa. B, and Ravi. S, 2005, "Database Security—Concepts, Approaches, and Challenges ", "IEEE Transactions on Dependable and Secure Computing", pp. 2-19
[30] Jason. D, 2004, "Defeating Overflow Attacks", "SANS Institute InfoSec Reading Room", pp. 1-30
[31] Joel. S, 2003, "Testing and comparing vulnerability analysis tools", "TechTarget", available at "http://searchsecurity.techtarget.com/Testing-and-comparing-vulnerability-analysis-tools" 2/5/2015
[32] Yue. Z, Serge. E, Lorrie. C and Jason. H, 2006, " Phinding Phish: Evaluating Anti-Phishing Tools", " Carnegie Mellon University / Human-Computer Interaction Institute by an authorized administrator of Research Showcase ", pp. 1-17
[33] Forrest. S, 2015, "Anti-Malware", "webopedia", available at "http://www.webopedia.com/TERM/A/anti-malware.html" 2/5/2015
[34] Sophos Ltd., "2015", available at https://www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx, 1/6/2015
[35] Alka. J and Sweta. J, 2010, "Database Intrusion Prevention cum Detection System with Appropriate Response", "International Journal of Information Technology and Knowledge Management", pp. 651-656
[36] Ionx Solutions LLP, 2015, "Verisys product", available at http://www.ionx.co.uk/solutions/file-integrity-monitoring 30/4/2015
[37] Mark. N, Avivah. L and Paul. E. P, 2009, "Pattern Discovery with Security Monitoring and Fraud Detection Technologies", "Gartner Inc.", pp. 1-10
[38] Entrust, Inc., 2007, "Understanding Digital Certificates & Secure Sockets Layer: A Fundamental Requirement for Internet Transactions", "Entrust, Securing Digital Identities & Information", pp. 1-11

Prof. Abdel Nasser H. Zaied, is prof. of Information Systems, Dean, Faculty of Computers and Informatics, Zagazig University, Egypt. He previously worked as an associate professor of Industrial Engineering, Zagazig University Egypt, an assistant professor of Technology Management, Arabian Gulf University, Bahrain; and as visiting professor at Oakland University, USA. He supervised 12 PhD. thesis and 45 MSc. thesis, and examined 8 PhD. thesis and 47 MSc thesis. He published 30 research papers in International and Regional Journals and 22 research papers in International and National conferences. His areas of research are: Systems Analysis and Design; Information Security; Knowledge Management; Quality Management Systems, Information Security and project Management, Electronic applications.

Prof. Walid I. Khedr is an associate professor of Information Technology, Head of Information Technology department, Faculty of Computers and Informatics, Zagazig University, Egypt. His current research interests are primarily in network security protocols, cryptography, key management protocols, and RFID security. Another field of interest is quantum cryptography.

Shimaa S. Mohamed is a Lecturer of Decision Support Systems and MSc. candidate, Faculty of Computers and Informatics, Zagazig University, Egypt.