Common Database System Vulnerabilities: A Risk and Mitigation Survey

Yash Shah
{shah_yash10@gatech.edu}
Georgia Institute of Technology

Abstract

Database is an integral backbone of any and all organizations. The information they hold are vast and often sensitive in nature. With the increasing activities in cybercrime, the unauthorized access to database systems through criminal means is an ever increasing concern and the risk factor associated with data and database systems are constantly increasing. To this extent, this paper introduces some of the principal database vulnerabilities, their mitigation guidelines and explore the possible effects of exploitation of said vulnerabilities. For the vulnerability discussed a possible threat vector is exposed and threat mitigation tactics are discussed. Further discussion takes place about statistics related to the incidents/data breaches in private sectors and related costs and losses are explored.

I. Introduction

As organizations increase their reliance on, possibly distributed, information systems for daily business needs. They become more vulnerable to security breaches even as they gain productivity and efficiency advantages. Though a number of techniques, such as encryption and electronic signatures, are currently available to protect data when transmitted across sites, a truly comprehensive approach for data protection must also include mechanisms for enforcing access control policies based on data contents. Also, techniques for data integrity and availability specifically tailored to database systems must be adopted. In this respect, over the years the database security community has developed a number of different techniques and approaches to assure data confidentiality, integrity, and availability. However, despite such advances, the database security area faces several new challenges. Factors such as the evolution of security concerns, new computing paradigms and applications, such as grid-based computing, on-demand business and distributed systems and databases, have introduced both new security requirements and new contexts in which to apply and possibly extend current approaches. To this effect it becomes imperative to analyze some of the more common databases threats, their utilization scenarios, possible mitigation techniques and the effects of databases breaches on business enterprises.

Security reports released by principal security firms, like OWASP, Symantec, Imperva, [10][6] state that database vulnerabilities are the prime target for exploitation in order to bypass defense of targets. The Imperva security firm recently issued a report about the principal database vulnerabilities for enterprises.

Using this and similar reports a list of the top database security threats has been compounded below [1][6]:

1. Excessive privilege abuse
2. Legitimate privilege abuse
3. Privilege elevation
4. Exploitation of vulnerable, misconfigured databases
5. Database communication protocol vulnerabilities
6. SQL injection
7. Malware
8. Denial of service
9. Unauthorized copies of sensitive data
10. Backup data exposures

II. Threats and their Analysis

Though the above list might seem obvious at a glance, many IT technicians still ignore many of them and the success of so many attacks against enterprises and organizations is a demonstration of this fact. The above security threats are clustered into groups and discussed below in a more detailed manner.

2.1. Privilege Abuse and Escalation

The first three points in the above list are related to the abuse of database privilege settings. In the case of ‘legitimate privilege’ and ‘excessive privilege’, the principal source of threat is represented by the grant of unnecessary access privileges to the users or applications with consequent increase of the attack surface. In the third case, the threat is represented by the unauthorized escalation/elevation of privilege for malicious reasons.

The mitigation for this category of database vulnerabilities is the elimination of any excessive rights; of course, this requires an additional effort for administrators who would have to identify the access rights for each user based on their real business needs. This task could be executed manually, but is prohibitively time-consuming. For this reason large enterprises deploy access control specific solutions for analytical processes.

The access rights could be managed at various levels like:

- Control of query-level access discriminating SQL operations

(SELECT, UPDATE, etc.) and data for each entity that access to the system. Query-level access control is useful not only for detecting excessive privilege abuse by malicious employees, but also for preventing most of the other top ten threats described herein[6].

- Another element to consider is the exploit of legitimate privileges that could be abused by ill-intentioned users for obtaining access to corporate database. It is possible, for example, that malware on the machine could catch the database credentials to retrieve information stored in the archive.

A possible solution to legitimate privilege abuse is the deployment of the context of database access controls enforcing policy for client applications, time of day, and location. In this way, it is possible to discriminate the use for legitimate database access privileges.

2.2. Misconfigured Databases and Leak of Input Validation

Unpatched databases, misconfigured archives still having default accounts and configuration parameters are prime exploitable vulnerabilities. The first step of penetration testing is the analysis of those flaws[4].

An efficient patch management process, especially for large enterprises, could reduce the time of exposure for the release of new database patches; vulnerability assessment activities could also support the mitigation of these cyber threats.

2.3. Denial of Service (DoS) and Database Communications Protocol Vulnerabilities

Like any other service, a database can suffer a denial of service attack. DoS may be achieved by exploiting database platform vulnerabilities to crash a server, flooding the system with requests, or using specifically designed malware.

Protection from these cyber threats needs a multiple level defense system that has the capability to recognize the sources of attack and apply the needed countermeasures. It’s fundamental to put in place defensive measures at network, application, and database level.

Another critical element for database security is represented by a communications protocol that could be exploited by attackers to obtain unauthorized access to the data. The principal database vendors are aware of cyber threats related to the communication protocols. Most of the recent security fixes released by IBM and Oracle are largely related to protocol vulnerability [7].

The countermeasure most efficient against database communication protocol attacks is protocol validation designed to parse traffic and block malicious ones in case anomalous patterns are detected.

[NOTE: The SQL Slammer2 worm represents a perfect example of malicious code designed to exploit a flaw in Microsoft service.]

2.4. Backup Data Exposure

Backup Data exposure could be caused by various factors. For example, it is possible that data backup devices are stolen or unauthorized copies of sensitive data are accessed by unauthorized entities. The principal cause of data exposure is the absence of a secure mechanism for protecting database copies. In many cases, companies that were victims of incidents did not have an inventory of all their databases and related backups. Each database is a mine of information and could contain sensitive data that need the control of accesses [4][8]. Outdated database instances represent one of the principal weaknesses for organizations. Numerous security audits revealed the absence of proper management of media containing old copy of the databases.

To mitigate data leaks through backup data exposure, a company must identify all databases within internal infrastructures and the data contained, for each archive it has to define privileges of access and maintain track of every activity during its lifecycle, from its creation to the dispose of the media support used for the storage.

Data classification is also necessary identifying the sensitive information within the archives. This can be used in the discovery of combinations of data that could expose confidential information, despite the fact that the same data could appear innocuous, if combined they could reveal sensitive data. An accurate inventory of databases including location of sensitive data and access controls should be set in compliance with corporate data access policies. To prevent backup data exposure it is also necessary to encrypt the backup.

2.5. SQL Injection

The SQL injection is probably the most popular vector of attack for databases. In a typical attack, the hackers inject unauthorized database statements into a vulnerable SQL data channel, such as stored procedures and web application input parameters. These injected statements are specifically crafted to be executed on the database side for malicious purposes. The successfully execution of a SQL injection attack can give to the attackers unrestricted access to an entire database. If these injected statements are executed by the database, critical data stores can be viewed, copied, and altered.

Three techniques can be combined to effectively combat SQL injection: intrusion prevention (IPS), query-level access control (see excessive privilege abuse), and event correlation [10]. IPS can identify signatures for vulnerable stored procedures or SQL injection strings. By correlating a SQL injection signature with another violation, such as a query-level access control violation, a real attack can be identified with extreme accuracy as the probability that a SQL injection signature and another violation would appear in the same request during normal business operation is extremely low.

2.6. Malware and Databases

A serious threat for the database is represented by the most classic cyber threat, malware. Malware authors tailor malicious code to automate the exploitation of one of the above points for specific database systems. The principal purposes of such malicious agents are information stealing and sabotage. As the damage to an enterprise database could have serious repercussion on business for private companies. One of most popular agents that targeted victims' databases is W32.Disttrack malware [9], also known as Shamoon, which is able to wipe out data from infected hard disks.

In November 2012, Symantec published a security alert on a new malware dubbed W32.Narilam that was designed to damage corporate databases. But unlike Shamoon, this malware was tailored to be active only within a specific geographic areas, the Middle East [3].

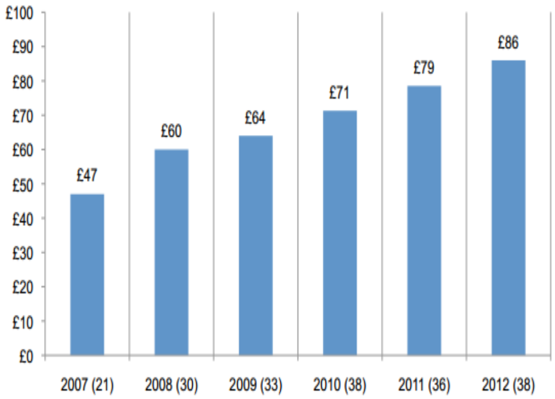
Unless appropriate backups are in place, the affected database will be difficult to restore. The affected organization will likely suffer significant disruption and even financial loss while restoring the database. Thus a constant anti-virus updates and scans are necessary in addition to frequent database backup to minimize data loss.

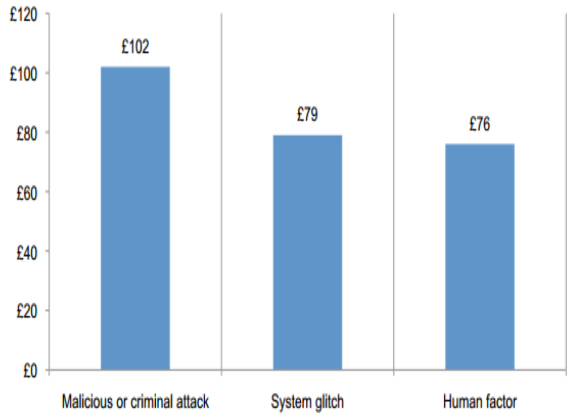
III. The Cost of a Data Breach in Private Sector

Now we have listed the principal vulnerabilities related to a database. Unfortunately, the cost related to a data breach is still very high and its analysis it is necessary to highlight the importance of adopting proper countermeasures to mitigate the risk of incidents cyber-attacks.

A study by Symantec [2] focused on the cost of data breach incidents for companies located in the UK examines the costs incurred by 38 companies in 12 industry sectors after these businesses experienced the loss or theft of protected personal data and then had to notify breach victims and/or regulators as required by law. The average per capita cost of an incident increased from £79 to £86 (all figures are in millions) and the cost of data breach continues to rise for the sixth consecutive year for all companies.

Figure 3 – Total organizational cost of data breach [2]   Figure 5 –root causes and cost of data breach [2]





The organizational cost grew from £1.75 million to £2.04 million. Negligence is considered the main cause of data breaches (accounting for 37% of incidents) [2], confirming the need to establish a strong commitment for the diffusion of security culture within corporates. The study also revealed the increase in malicious attacks from 31% to 34%, and related data breaches are generally considered most costly.

Lost business cost has nearly doubled over the last six years, also ex-poste response and detection costs (e.g., activities that attempt to address victims', regulators', and plaintiff counsels' concerns about the breach incident, legal and consulting fees that attempt to reduce business risk and liability) increased from approximately £451 thousand in 2011 to £508 thousand in 2012 [2].

IV. Conclusions

The data presented above demonstrate how expensive cyber threats that target vulnerabilities in databases can be. Despite the high level of awareness of the principal menaces, the number of incidents has only increased in recent years along with the costs suffered by victims of these incidents.

To reduce the impact of these events, an organization needs to prepare a formal incident response plan as the adoption of proper procedures could, in fact, reduce the total cost of a data breach. Organizations have to define and adopt a strong security policy sustained by a strong commitment of higher management and the policy must include corporate database security. The hiring of outside security consultants could also contribute to the improvement of both policy definitions and breach investigation. But despite all of this, the data related to the breach incidents seems to suggest that organizations still don't perceive the ever increasing threats associated with it.

V. REFERENCES

[1] 'Top Database Security Threats: The Most Significant Risks of 2015 and How to Mitigate them' - Worldwide Security Products, 2015 (White paper)

[2] '2013 - Cost of Data Breach Study' - Symantec and Ponemon Institute LLC, 2013

[3] 'WORM_NARILAM.A/B – Rapid Release and Daily Certified virus definitions' – Masaki Suenaga and Alan Neville, Symantec Corporation, 2012

[4] Database security: Concepts, Approaches and Challenges – Bertino et al, IEEE transaction on dependable and secure computing, 2005

[5] 'Database Security: Research and Practice' - Bertino et al, Elsevier ScienceDirect, 1995

[6] 'Top Ten Database Security Threats' - Amichai Shulman, CTO Imperva, Inc., 2014 (White Paper)

[7] 'Vulnerability Update August, September, October 2014' - Secunia Inc. Incident Report

[8] 'Database security: threats and challenges' – Rohilla et al, International Journal of Advanced Research in Computer Science and Software Engineering, 2013

APPENDIX A
SQL INJECTIONS

Malicious attackers successfully use SQL injection on legitimate web sites using various techniques: They often adopt a search engine's index to find vulnerable websites by using one of the numerous DIY SQL injecting tools available on the black market, like DIY Google Dorks based hacking tool. The tool relies on Google Dorks for a target evaluation. In particular, the DIY Google Dorks based hacking tool has built-in features that can be used to evaluate the possibility of performing a SQL injection attack or to discover all the targets that aren't protected by a CAPTCHA challenge mechanism.

Example: Let's use a very simple query as example: ***SELECT fields FROM myTable WHERE field = '$EMAIL';***

Where $EMAIL' is an email address provided by the user via a web form. If an ill-intentioned user provides the following input:

<***dummy’ OR ‘1’ = ’1***>

in the email field, and it is not validated, the resulting SQL will be:

SELECT fields FROM myTable WHERE field = 'dummy’ OR ‘1’=’1';

Due the presence of the ‘1’=’1′ condition, which is always TRUE, the query returns every item in the myTable.

APPENDIX B
NARILAM WORM

The W32.Narilam worm attempts to spread by copying itself to all drives and certain shared folders on the victims system. There weren’t instances that included a module to steal information from the victims.

The worm was designed to attack SQL archives; it was able to search for database instances having one of the following names:

Alim, Maliran, Shahd (Arabic/Persian Db names used commonly). Once the database instance was found, the malware was able to access database objects to manipulate them; it was also able to delete the entire archive. The malware was designed to find objects with specific names belonging to the Arabic and Persian languages (e.g., hesabjari than means “current account” in Arabic/Persian). Narilam was written in the Delphi programming language and has a behavior similar to other malicious agents. The investigation revealed that the malicious code was designed to target mainly corporations, the percentage of business users hit is of 97.1%, while non-business users are at 2.9%.