Database Security

Catherine Boothman, Oisin De Conduin, Eoin Gillen,
Sean Nolan, John Cahill, Mairtin Mac Colgain

October 18, 2013

Abstract

Database technology has changed over the years and with the advent of cloud computing and web based storage Database Management Systems (DBMS) have become affordable to small business and organisations that would have tradionally been far to small to cover the cost of one. As more and more of these businesses and organisations rely on database technology to store the information critical to their day to day operation, the security of these databases has become an increasingly more complex and important issue. The traditional problems associated with databases was the loss of data through physical damage to the on-site database server and making sure employees had correct and appropriate access to relevant data only. There was minimal, although not negligible, risk of non-authorized access from non-company personnel and damage to a database through internet connections. However as cloud based DBMS solutions became available, both as a backup to large companies and as an affordable option to others, far more must be done to keep data safe. This paper outlines the common threats facing databases and the measures taken where possible to project against them and mitigate any potenital risk to data from them.

1 Introduction

Databases and database systems have become a major part of everyday life in modern society. Nearly everything we interact with and depend on have some kind of dependence on a database [1]. From taking money out of the bank, to paying tax and ordering products online. For decades at this point nearly every business has made use of some kind of database technology to manage employee records, customer details, product and supplier details. These are the critical functions of a business and yet they are the simplest and oldest uses of a database. With the advent of web based applications and information systems technology, the potential use of databases to businesses and, consequently, the reliance of businesses on them has exploded. Never before has security been such a major issue. Cloud storage and applications open up sufficient space and processing power to smaller businesses and social organisations who would not have had the turnover for the cost of a traditional DBMS housed on-site. However with this technology a whole new set of security risks have been introduced by exposing companies' private data to the potentially public world of the world wide web.

Security threats can be roughly categorised into the following three areas; 1) unauthorized data observation, 2) incorrect data modification, and 3) data unavailability. All businesses and organisations may suffer heavy financial and reputational losses due to unauthorized data observation. Incorrect modifications of data, either intentional or unintentional, result in an incorrect database state and the use of incorrect data may in turn lead to heavy losses. When data is unavailable, crucial information for the proper functioning of a business or organisation is not readily available when needed [2], just ask anyone who had an Ulster bank account last year how annoying that is!

Therefore in order for a database to be considered secure the following requirements must be met. 1) Data privacy protection data against unauthorized disclosure, sometimes referred to as secrecy or confidentiality. 2) Data integrity refers to the prevention of unauthorized and improper data modification. 3) Data availability refers to the prevention and recovery from hardware and software errors or physical damage and from malicious data access denials making the database system unavailable. These three requirements arise in practically all application environments [2]&[3] and will be dealt with in more detail later in this paper.

2 Threats To Database Security

2.1 Human Error

One of the biggest threats to database security is from authorised users who do not follow proper safety protocol because of a lack of education or carelessness; this can lead to 'Authentication Errors' [3]. Errors by users include;

- Leaving a computer logged in while unattended, for example: if going out for lunch a user does not lock computer.
- Weak password - Use of common or simple password making it easy for hackers to guess.
- Visiting illegitimate websites or downloading malicious attachments.
- Illegitimate disclosure of information, such as a password, to unauthorised personnel [14].

Email, instant messaging and Social Networks are the most common means of virus spread. Social engineering is used to convince users to open an email, click on a link or possibly even download an attachment, opening up a database to harm. Phishing is a form of email attack that uses social engineering to convince users to hand sensitive information over to a cracker, such as a password, which they can then use to attack databases[14].

Nonrepudiation methods should be used to track users' access and manipulation of a database, so if there is an error or attack it will be able to be traced back to a particular user account [3].

2.2 Malware Attack

Although Databases can be configured to only allow local access, increasingly they are placed on the cloud or a specific server, with access allowed through the internet or across a network. This openness creates possible security threats from malicious planned computer attacks over the network. Furthermore, increasingly important business, financial and personal information is uploaded into Databases, making them enticing and profitable targets for intruders [14].

There are over 600,000 malware programs at large on the internet. Malware is a term for malicious software that is designed by intruders to carry out unauthorized activity on a computer or network, these can often be damaging of destructive to a database[14].

Malware comes in the following forms;

2.2.1 Viruses/Trojans/Worms/Spyware/Bots

Viruses are self-replicating pieces of software that install themselves on a computer without user consent. Once installed, they can often carry out harmful attacks on databases. They can access private information, log keystrokes, corrupt/manipulate data, along with numerous other harmful acts [14].

Trojans are malicious programs that disguise themselves as legitimate programs. Unlike viruses they do not replicate. They can be used to harm/manipulate databases or carry out other remote attacks[14].

Worms can be seen as a specialist version of virus, with the major added danger that they do not need user input to travel through

a computer network. Worms are self-learning and will use information on vulnerabilities they found on one computer to infect the next computer on a network, potentially harming databases if programmed to do so[14].

Spyware is a type of virus that monitors your computer/database to steal your information without your knowledge. The information is sent back to the Spyware creator to use as they wish[14].

Bots are malicious programs that install themselves on your computer with the intent of controlling it. Bots are controlled by a cracker who may be able to control thousands of computers by infecting them all with Bots. Bots can be used for a Denial of Service (DOS) attack, where they flood a CPU with requests, slowing it down till it becomes unusable, or else doing the same to a network or database, to shut it down[14].

2.2.2 SQL Injection

SQL injection is a particular danger to databases and other data driven systems. It involves malicious SQL statements being inserted into the entry field of a database and then executed. Hijacking website URLs and sending information through a web-browser is a common attack "vector". SQL injections can be used to reveal confidential database information to an attacker, or carry out unauthorised manipulation of a database, causing harm to a database [14].

2.3 Natural Disasters

Natural Disasters present an uncontrollable threat to the data centers and databases, such incidents include earthquakes, flooding, Hurricanes and fire.The threat presented is twofold there is an immediate threat to any equipment and data present there is also the threat of service downtime. if the databases is critical to a number of onsite or even offsite services any downtime can result in a loss of revenue and customer confidence.

When preventing to attempt damage to data base systems response time is crucial. a fire , for example can spread quickly through a data centre; causing damage to equipment and endangering personnel. Given the risk associated with a fire, any attempts to tackle a large fire will be carried out by emergency services.This small window is enough time for a fire to cause massive damage to a data centers equipment and to potentially destroy any on site backups.

While Natural Disasters may not necessarily damage the data centre itself it can damage the infrastructure in the surrounding area, as such it is important to keep access to power and telecoms as long as possible .Redundant services may also be used to keep the database up and running

A recent example of data systems caught in the area of a natural disaster can be seen in the New York area during 2012's Hurricane Sandy.The hurricane itself resulted in a number of data centers in the manhattan area being cut off from power and in some cases telecoms; the subsequent flooding led to damage of essential equipment and services which brought databases offline for a number of weeks until a restoration effort could be carried out.[8]

2.4 Hardware Failure

Given that most databases will run on a continous basis Hardware failure is an expected consequences of operating a data center.There are a number of hardware copmonents which can fail in a database including Memory,CPU's motherboards and power supplies[13].However the most common component failure comes from hard drives.

Mechanical storage is the most cost effective method for storing large volumes of data on a non volatile medium[7]. Due to the drives structure and moving parts, they are prone to failure as they age.

2.5 Human element

While the security risks dicsussed above primarily deal with elements outside of control there are physical risks to a data center /data base which can come from a human element, these can range from the unitentional to the malicious.

Encryption of data will make it difficult to glean any sensitive information from stolen hard drives;data bases and larger Data Centres can contain a myriad of high value equipment.This equipment can range from complex networking equipment such as servers and network switches to fibre cable and tools.

Equipment can also be damaged during a break-in ; one such break-in occurred in Vodafone's Basingstoke data center in the United Kingdom [12]. Thieves caused damage to a number of servers resulting a service outage to Vodafone's voice SMS and internet services.

It is also possible for elements within an organization to present a threat to a database. Sabotage of a database or falsification of the data stored on it by employees for malicious purposes disruption of services and a loss of data integrity. These acts can be carried out for the purposes of committing fraud or can be purely destructive.It is important to ensure an adequate security system is in place alongside restricting access to only essential staff.

Trojans are malicious programs that disguise themselves as legitimate programs. Unlike viruses they do not replicate. They can be used to harm/manipulate databases or carry out other remote attacks [14].

Worms can be seen as a specialist version of virus, with the major added danger that they do not need user input to travel through a computer network. Worms are self-learning and will use information on vulnerabilities they found on one computer to infect the next computer on a network, potentially harming databases if programmed to do so [14].

Spyware is a type of virus that monitors your computer/database to steal your information without your knowledge. The information is sent back to the Spyware creator to use as they wish [14].

Bots are malicious programs that install themselves on your computer with the intent of controlling it. Bots are controlled by a cracker who may be able to control thousands of computers by infecting them all with Bots. Bots can be used for a Denial of Service (DOS) attack, where they flood a CPU with requests, slowing it down till it becomes unusable, or else doing the same to a network or database, to shut it down [14].

3 Security Measures

3.1 Physical Risks

3.1.1 RAID

One of the easiest and most common ways to protect a database against hard-drive failure is to use RAID (redundant array of independent disks) [15] This is an umbrella term used to describe data storage schemes that divide and replicate data across multiple hard drives in real time. This allows a server to use mutliple hard drives at once, increasing performance and allowing for easy data recovery in case of hard drive failure.

3.1.2 Off-site backups

However in the even of a flood/fire or other disaster, an entire server could be destroyed. On of the many ways to secure a backup of a database system against these possible physical risks is to keep a secure off-site backup away from the main site. This way, even if the site of the main server is compromised, it is possible to recover the data from the off-site backup.

3.1.3 Cloud storage

Storing a backup in the cloud allows for recovery, similar to storage on an off-site location. Keeping sensitive data in the cloud may not be as secure as keeping it in a separate off-site location [16], though it may be more convenient.

3.2 Human Error

3.2.1 Role-Based Access control

The most straightforward way to protect a database against human error is to control access to the database tightly.Applying the principle of least privilege, make sure that people only have access to the areas of the database that they need, and nothing more.The challenges include handling multiple roles, conflicting roles and consistency of the access control roles.

3.2.2 Testing

The fault-tolerance computing community has come up with several algorithms for recovering databases and systems from failures and other problems .These techniques included acceptance testing and checkpointing [3]. Sometimes data is replicated as aforementioned so that there are backup copies. Therfore it is imperative to make sure that all code is checked and tested before it goes live. A single bug could be enough to take down an entire system, so proper testing is needed to ensure there is no problems that could compromise the integrity of the database.we also need flexible security policies as the requirements such as security and real time processing may be conflicting [3].

3.2.3 Risk Analysis

Before developing any computer system for a particular operation, one needs to study the security risks involved.The goal is to mitigate the risks or at least limit and contain them if the threats cannot be eliminated. The challenges include identifying all the threats that are inherent to a particular situation. This is especially useful for viruses as once a virus starts spreading, the challenge is how do you stop it or if you cannot how do you contain it and limit the damage the that is caused [3]? Although various AntiVirus software packages will possibly limit the virus from affecting the system or causing serious damage new viruses are being developed all of the time and therefore it would be prudent to stay one step ahead.

3.3 Malicious Risks

3.3.1 Firewalls

Various Organisations now have web infrastructure for internal and external use. To access the external infrastructure one has to go through the firewall. These Firewalls examine the information that comes into and out of an organisation. This way the internal assets are protected and inappropriate information may be prevented from coming into an organisation [3]. It is also possible to throttle connections through the firwewall to increase security and reduce access to database servers.

3.3.2 Data Mining

Data mining is the process of posing queries and extracting patterns, often previously unknown, from large quantities of data using pattern matching or other reasoning techniques. Data mining may be used to detect and possibly prevent cyber-attacks. For example, anomoly detection techniques could be used to detect unusual patterns and behaviours. Link analysis may be used to trace the viruses to the perpretrators. Classification may be used to group various cyber-attacks and then use the profiles to detect an attack when it occurs. Prediction may be used to determine potential future attacks. data mining can aslo be used for analyzing Web logs as well as analyzing the audit trails. Based on the results of the data-mining tool, one can then determine whether any unauthorised queries have been posed [3]. It is important also to note that Data mining gives out information not previously known using various reasoning techniques such as statistical inference which exacerrbates the Inference problem whereby unauthorised information can be deduced from legitimate resonses to queries posed.This needs to be considered and approriate security and privacy constraints applied to all data sources.

3.3.3 Protecting information

While ideally the information in a database should never be compromised, sometimes there is no amount of preparation that can stop it. Even the biggest companies with high-end security can be breached, such as with Sony and the Playstation Network [17]. In cases like these, it is imporant that all sensitive data be encrypted in some way.

Passwords and other information can be encrypted using a hashing algorithm. This takes a block of data and returns a fixed-length string called the hash-value. Even a single character changing in the data block will return a completely different hash value. As such, it is possible to store this hash value instead of the actual password, so even if a database is compromised, all the attackers get is a list of encrypted passwords. For other types of information, using hash functions on for example a message, a message digest is created. If appropriate functions are used each message will have a unique digest.Therefore even a small modification to the message will result in a completely different message digest. this way integrity is maintained. Message digests together with cryptographic receipts, which are digitally signed, ensure the receiver knows the identity of the sender [3].

It is however possible to reverse engineer the passwords from the hashed values if the hashing algorithm is known. This can be done using a dictionary attack, or something similar. To prevent this, passwords can also be salted before they are hashed, by inserting random characters into the password [18].

3.3.4 Database hardening

It is extremely important to keep up to date with patches as indicated by the SQL Slammer Worm which affected circa 100,000 systems in January 2003 exploiting the buffer overflow problem. The worm was made possible by a software security vulnerability in SQL Server first reported by Microsoft on July 24, 2002. A patch had been available from Microsoft for six months prior to the worm's launch, but many installations had not been patched. Furthermore stored procedures and triggers can lead to privilege escalation and compromise and this should be considered prior to establishing.Databases Finally database processes should be run under dedicated non-privileged accounts through applications and unneeded components of said databases disabled.

References

[1] Ramez Elmasri and Shamkant B. Navathe, *Fundementals of Database Systems, 4th Edition*, Pearson (2004)

[2] Elisa Bertino and Ravi Sandhu, *Database Security - Concepts, Approaches and Challenges* IEEE Transactions on Dependable and Secure Computing **2**, (2005)

[3] Bhavani Thuraisingham, *Database and Applications Security*, Auerbach (2005)

[4] Amichai Shulman, *Top Ten Database Security Threats: How to Mitigate the Most Significant Database Vulnerabilities*, Imperva Website

[5] Sumit Jeloka, Don Gosselin and Richard Smith, *Oracle®Database Security Guide, Release 2*, Oracle and/or its affiliates (2012)

[6] `http://www.cableorganizer.com/articles/how-to-fireproof-your-server-room.html`

[7] `http://research.microsoft.com/en-us/um/people/navendu/papers/sigcomm11netwiser.pdf`

[8] `http://arstechnica.com/information-technology/2012/10/hurricane-sandy-takes-data-centers-offline-with-flooding-power-outages/`

[9] `http://arstechnica.com/information-technology/2012/11/how-one-nyc-data-center-survived-hurricane-sandy/`

[10] http://www.techrepublic.com/article/disaster-recovery-how-to-protect-your-systems-from-flood-threats/

[11] http://www.sans.org/reading-room/whitepapers/awareness/data-center-physical-security-checklist-416?show=data-center-physical-security-checklist-416\&cat=awareness

[12] http://www.computerworlduk.com/news/mobile-wireless/3262920/vodafone-in-network-outage-following-datacentre-break-in/

[13] http://www.datacenterknowledge.com/archives/2008/05/30/failure-rates-in-google-data-centers/

[14] Alfred Basta and Melissa Zgola, *Database Security*, Delmar Cengage Learning (2011)

[15] Donald, L. (2003). MCSA/MCSE 2006 JumpStart Computer and Network Basics (2nd ed.). Glasgow: SYBEX.

[16] Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.

[17] http://www.cbc.ca/news/technology/playstation-data-breach-deemed-in-top-5-ever-1.1059548

[18] http://www.dshield.org/diary.html?storyid=1111