Database Security

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

October 18, 2013

Abstract

This fantastic paper is all about database security and how important this is.

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 to ordering products on-line. 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 efficient space and processing power to smaller businesses and socail 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 Risks

2.1 Physical Risks

Along side malicious attacks physical attacks provide a threat to databases and datacentres. Unlike Malicious attacks, which are carried out intentionally physical threats can orig-

inate from a number of non human sources such as weather, hardware failure and infrastructure failure. The risk of human related elements is still present ranging from the accidental to the malicious. While these threats cannot be removed outright it is possible to mitigate them; and in the event of there occurence reduce their impact on Data loss and system downtime.

Environmental threats to databases covers a number of hazards including fire and natural disasters such as flooding, earthquakes and forest fires. These threats present a risk to a data centers hardware. The structural integrity of the building they are housed in and while an indirect threat access to services such as power, telecoms and environmental controls.

2.1.1 Fire

A fire in a data centre is a catastrophic event; resulting in damage to critical equipment and data loss as well as service downtime as repairs are carried out.

A Fire can spread quickly through a data centre; causing damage to equipment and endangering personell. 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.

Fires can be caused by a number of sources but by far the most common is faulty equipment or power cables [6]. It is important to ensure sources of ignition or potentionial fuel is kept away from any critical equipment.

2.1.2 Flooding

Flooding is an uncontrollable threat to data centres; A flood can cause damage to critical database equipment, services and even in extreme cases structural damage to the building itself. The damage caused can be mitigated through proper planning and preventative measures. Preventative measures to protect against flooding primarily consist of backing up data offsite and access to services. The key aims involved in preventative measures are to protect critcal data/equipment and to reduce the downtime experienced by clients to a minimum. In the event of a flood any physical medium such as tapes or hard drives may not be accessible depending on the severity of the flood; it is crucial that copies exist outside of the floodzone for easy recovery. This will allow for a faster recovery and until services are fully restored will allow the clients to make alternative arrangments to reduce downtime to their business.

While flooding may not nessecarily damage the datacentre 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. Data centre will keep a series of backup generators and a reserve of fuel to allow them to function independent from the local power grid. While this reserve will not be sufficient to run the centre for an extended period of time it will provide a window in which steps can be taken to ensure all critical data can be backed up and saved.

The second stage of flood measures is to protect any critical equipment such as server racks and UPS's from damage. It is important to ensure that as much equipment as possible remains above the water; depending on the equipments location in the building this may not be possible. Equipment can be covered in plastic tarp to help reduce water damage but this is by no means a fool proof solution, after flood waters have receded recovery of the data centre can begin. The first step is to salvage as much equipment as possible and replace any damaged equipment; after the physical system is restored data can then be reloaded onto the systems from the offsite backups.

A recent example of datacentres which where damaged during flooding occured during hurrucane Sandy. Data Centres were cut off from services and in some cases had to run as long as twelve days on reserve fuel before services were restored [8].

2.1.3 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 supplys [13]. However the most common component failure comes from hard drives.

Mechanincal 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 more prone to suffer failures than other alternatives such as solid state drives.

Given the possibility of failure associated with hardware it is paramount that a database be backed up routinely. Hard drive integrity can be increased using techniques such as RAID arrays, which will allow data to be rebuilt from a cluster of Hard drives should one fail. Other hardware should be swapped out as soon as the failure arises to ensure a minimum of downtime for the database. A proactive maintaince schedule will help to reduce the impact of hardware failure on the database.

2.1.4 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 occured in vodafones Basingstoke data center in the United Kingdom [12]. Thieves caused damage to a number of servers resulting a service outage to Vodafones voice SMS and internet services.

It is important to ensure an adequate security system is in place alongside restricting access to only essential staff.

2.1.5 Services Failure

For a database to be operational it requires the support of essential services which may provided by an outside organization. Failure of services such as power and telecommunications can result in service downtimes and potential loss of data. Failure of power and telecoms can occur as a failure on the service providers end; it can also occur as a result of the data centre overstressing the services available is important for a DBA to consider the power and Bandwidth requirements of their system, Power Distribution Units(PDUS) and there are a number of software solutions which can monitor bandwidth usage.

2.2 Human Error

One of the biggest threats to computer network security is from authorised users who do not follow proper safety protocol because of a lack of education or carelessness. 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.

Email is one of the most common means of virus spread. Social engineering is used to convince users to open an email and possibly even an extra attachment. Malicious code can be in

HTML form or any type of code can be used in the attachment.

Phishing is another form of email attack that uses social engineering to convince users to hand sensitive information over to a cracker, which they can then use to attack networks and databases.

Instant messages and social networks, like Twitter, are a relatively new route for malicious attacks. Crackers will again use social engineering to convince users to click on illegitimate links or download malicious software, opening up a network or database to harm [14].

2.3 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.

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.

Malware comes in the following forms;

2.3.1 Viruses

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, such as stealing memory or CPU activity. They can be very dangerous if they are designed to steal or harm databases. They can access private information, log keystrokes, corrupt/manipulate data, along with numerous other harmful acts.

Crackers can be very smart about designing viruses to exploit specific security vulnerabilities or use social engineering to fool users into downloading malicious packages. There are many different types of virus, such as File-infected viruses and Multipartite viruses [14].

2.3.2 Trojans

Trojans are malicious programs that disguise themselves as legitimate programs. Unlike viruses they do not replicate. They are used to gain access or cause harm to a computer or network. There are numerous different types of Trojan [14].

2.3.3 Worms

Worms can be seen as a specialist version of virus, with the major added danger that they do not need user input to travel from one computer to another. They are programmed to automatically exploit networks(internet or LAN) and travel from linked device to linked device. Worms are self-learning and will use information on vulnerabilities they found on one computer to infect the next computer on a network. A worm will repeat the pattern of infecting, learning and spreading until it has potentially destroyed a whole network [14].

2.3.4 Spyware

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

2.3.5 Adware

Adware is like spyware as it can gather information on a user without consent, but it can also be used to display targeted ads to a user, often through the form of pop-up web pages [14].

2.3.6 Bots

Bots are malicious programs that install themselves on your computer with the intent of controlling it. Bots can carry out a wide array

of functions. Bots are controlled by a cracker who may be able to control thousands of computers by infecting them all with Bots. Together these infected and controlled computers are now called a Botnet.

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. They can also be used by their creator to carry out illegal acts like DOS or phishing attacks on other targets. Bots are difficult to find and hard to remove, often needing the whole OS to be reinstalled so a user can be sure their computer is Bot free [14].

2.3.7 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].

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 Access control

The most straightforward way to protect a database against human error is to control access to the database tightly. Make sure that people only have access to the areas of the database that they need, and nothing more.

3.2.2 Testing

Another way to protect the database is to make sure 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.

3.3 Malicious Risks

3.3.1 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.

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]

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/ 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=11110