ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

Database Security and Confidentiality

Ms.Gurpreet Kaur Sodhi

Assistant Professor, University Institute of Computing (UIC), Chandigarh University, Gharaun, Mohali , India

Abstract: Database security is a main challenge these days. Companies store sensitive information in databases, however, database security is sometimes not given as much attention and effort as other areas of computer security. These databases can be easily hacked to obtain sensitive information. In this paper, I present two main aspects of Database security- security as most people would understand it (security from outside attacks) and security from the inside (confidentiality policies).

Keywords*:* Databases, security, confidentiality, technology.

I. INTRODUCTION

Database security is a double-sided matter, especially in modern times. People who monitor, use and repair databases need to be aware at all times that they have to monitor database security from both ends; databases are vulnerable from the breaking of confidentiality within the companies which use them as well as being vulnerable from the more well-known hacks from outside sources.

According to Duncan, Keller-McNulty and Stokes [1], companies have an obligation to protect the data they keep from misuse and\or accidental destruction while they hold it. This internal view is one which is not often thought about in the public sphere – the popular image of database security is more likely to involve the work done by Almutairi and Alruwaili [2], who focus on keeping data safe from outside intervention.

Database security as a whole is something which is becoming more and more of an issue as increasing digitalisation means that, not only is more and more information being committed to a digital format, but hackers and other people who would steal the information are gaining access to new technologies in their search for ways into databases.

II. DATABASE SECURITY : THE IDEAL SOLUTION

According to Almutairi and Alruwaili, "The objective of database security is to protect database from accidental or intentional los [SIC]"[1](pp.9), this gives us a deeper look into the types of security that we are ostensibly familiar with. In effect, we could say that when the double-sided equation of database security is broken down, each arm itself has multiple sides.

The two sides of protecting databases from the outside comes in the form of protecting them from malicious attack, and protecting them from the types of attack that would wipe the data from whatever server was holding it – for example an attack by a virus which managed to get through whatever defences the systems had in place, other aspect is to strengthen internal Data privacy policies.

To look at these sides in order, in order to protect databases from the types of malicious hacks they may face from rival companies, hackers, or simply people out to do whatever damage they can, there are several routes that companies and firms can take. To paraphrase Almutairi and Alruwaili, these routes include procedures in both the computing systems themselves and in the physical space which surrounds the servers and computers containing the data.

The physical space surrounding the hardware can be protected by the same measures which are used to protect databases from being used and abused by company or firm employees who don't have sanctioned access to the data contained in them. Since this is a subject covered more extensively by Dunan, Keller-McNulty and Stokes, we will focus more closely on it there.

The electronic space surrounding the databases, however, such as the company intranet and the whole wide electronic world which exists today can be strengthened by reliable firewalls and virus protection programs, both of which can be done strategically. Strong authentication models should be in place to avoid breaking of login credentials.

Duncan, Keller-McNulty and Stokes deal with the internal security of companies and firms which not only store information for their own research use but also " supply researchers and analysts with suitable data products"[1] as well. Having data moving through various electronic systems is of course a problem in itself, as Almutairi and Alruwairi have pointed out, but having sensitive data easily accessible through various interface points can lead to its own problems.

The examples of companies which might handle and spread data used by Duncan, Keller-McNulty and Stokes include data archives as the National Data Archive for Child Abuse and Neglect at Cornell and credit bureaus such as Experian. Since the data used by these types of organisations is necessarily highly sensitive, the need for protection is strong.

Protection in this case would perhaps not be so strongly focused on outside people looking in, since the information is quite often shared between organisations and independent researchers anyway; rather, the focus would be on ensuring that nobody in each of the respective organisations was given access they were not cleared to have.

DOI 10.17148/IJARCCE.2015.4267

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

Restrictions would be placed on both physical access – whether that be to the actual space occupied by the servers which hold the data, or to computer terminals – and software access, which is to say access to the actual data itself via password, or access to it because you were seen as having a legitimate reason for needing access to the data, such as an academic researcher needing it for a book she was publishing.

III. CONCLUSION

The ways in which we look at database security are only part of the whole area which is covered by it. While everyone knows that databases would need firewalls and protection against viruses, since we are all increasingly aware of that as our societies become more and more dependent on technology, we are not so aware of the need to protect from attacks or misuse of the data from the inside.

Since the reputations of companies depend almost entirely on how safe they can keep their data, particularly when it comes to organisations which only exist to store and move data, they obviously have to expend more time and effort on ensuring that the data is kept safe from people who have no business accessing it, which can take many different forms.

REFERENCES

[1] G. T. Duncan, S. A. Keller-McNulty and S. L. Stokes, "Database Security and Confidentiality: Examining Disclosure Risk vs. Data Utility through the R-U Confidentiality Map" NISS, Technical Report no. 142, pp. 1-24, March 2004.
[2] H. Almutairi & A. H. Alruwaili, "Security in Database Systems" Global Journal of Computer Science and Technology Network, Web & Security vol. 12, pp. 9-14, 2012.
[3] H. Almutairi & A. H. Alruwaili, "Security in Database Systems" Global Journal of Computer Science and Technology Network, Web & Security vol. 12, pp. 9, 2012.
[4] G. T. Duncan, S. A. Keller-McNulty and S. L. Stokes, "Database Security and Confidentiality: Examining Disclosure Risk vs. Data Utility through the R-U Confidentiality Map" NISS, Technical Report no. 142, pp. 2, March 2004.