© 2014 IJIRT | Volume 1 Issue 6 | ISSN : 2349-6002

Database Security: Threats and Research

Vinay, Ranjeet Kumar
Student of Information Technology
Dronacharya College Of Engineering, Gurgaon

Abstract- Data is the most valuable and important asset in today's world as it is used in daily life from a single individual to the large organizations. As almost all organizations become dependent on access to their data over the internet, the need for adequate security measures is becoming more and more critical. Though number of techniques like encryption, digital signature, and firewall are used as security measures but problems are always there. The database is still not immune of penetration, insiders and successful intruders. One of the requirements for the protection of internal resources is access control to ensure that all accesses are authorized according to some specified policy. In this paper we will see various threats to database security mainly to access to database systems and present some important and effective techniques to check the threats.

Index Terms- attacks, database security, threats**.**

I. INTRODUCTION

Information is that the most useful plus in today's world because it is employed in day –to –day life from one individual to giant organizations. to create the retrieval and maintenance of information simple and economical it\'s hold on in an exceedingly info. Considering the importance of information it\'s essential to secure it. Security in today's world is one among of} the vital and difficult tasks that individuals face everywhere the globe in every side of their lives. Equally security in electronic world incorporates a nice significance. Protective the confidential/sensitive information hold on in an exceedingly repository is truly the info security. There are a unit varied security layers in an exceedingly info. These layers are: info administrator computer user, security officer, developer's associate degreed worker and security may be broken at any of those layers by an offender. Info security may be compromised by getting sensitive information, dynamical information or degrading handiness of the info. Over the last thirty years the knowledge technology setting have skilled several changes of evolution and also the info analysis community have tried to remain a step sooner than the future threats to the info security.

II. DATABASE SECURITY THREATS

2.1 SQL Injection:

In a SQL injection attack, associate degree offender usually inserts (or "injects") unauthorized SQL statements into a vulnerable SQL information channel. Usually targeted information channels embrace hold on procedures and internet application input parameters. These injected statements area unit then passed to the info wherever they\'re dead. For instance in an exceedingly internet application the user inserts a question rather than his name. Victimization SQL injection, attackers could gain unrestricted access to a whole info.

2.2Unpatched DBMS:

In database, as the vulnerabilities are kept changing that are being exploited by attackers, database vendors release patches so that sensitive information in databases remain protected from threats. Once these patches are released they should be patched immediately. If left un-patched, hackers can reverse engineer the patch, or can often find information online on how to exploit the un-patched vulnerabilities, leaving a DBMS even more vulnerable that before the patch was released.

2.3 Data association problem:

Occurs whenever two values seen together are classified at a higher level than the classification of either value individually. As an example, the list containing the names of all employees and the list containing all employee salaries are unclassified, while a combined list giving employee names with their salaries is classified.

2.4 Excessive Privilege Abuse:

When users (or applications) area unit granted info access privileges that exceed the necessities of their

job operate, these privileges is also abused for malicious purpose. for instance, a pc operator in a corporation needs solely the flexibility to alter worker contact data could make the most of excessive info update privileges to alter wage data..

III. DATABASE RESEARCH

Reviewing the database security related topics of this time reveals a heavy focus on refinement of access controls, privacy protection and efficient data encryption.

3.1 Privacy Protection:

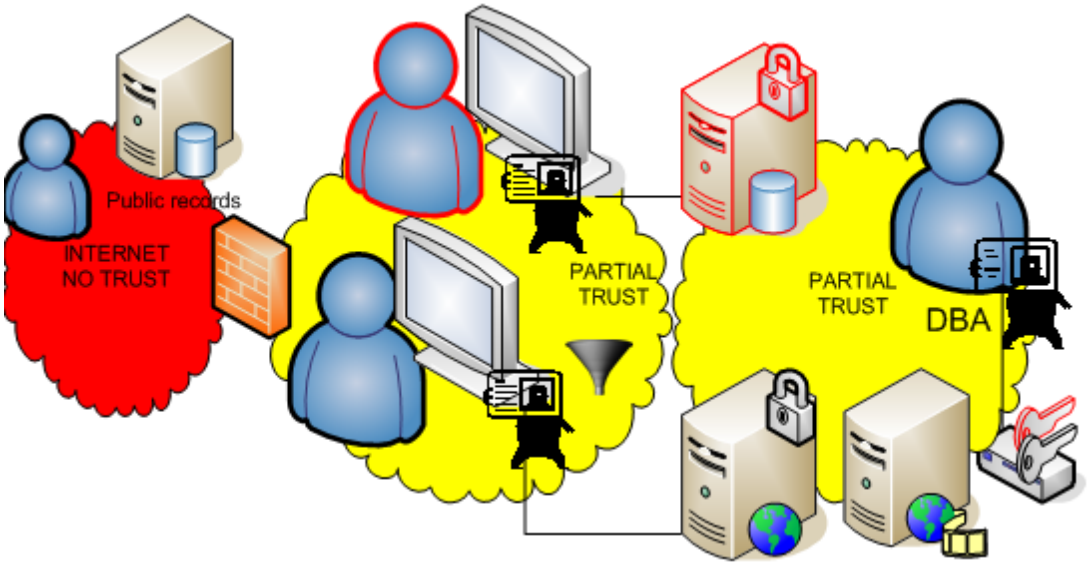
We have seen that reasoning drawback incorporates a long history in info analysis. Whereas up to 1990 these analysis centered on applied mathematics databases the introduction of information reposition amendment that. Simply before our fundamental quantity it had been shown that the final reasoning drawback was unsalable. In effect, the lot of reasoning controls were placed on the info it\'d become more and more unusable. These early analysis didn't\'t have to be compelled to concern itself with data processing from multiple sources. Many alternative techniques were introduced to touch upon this drawback that allowed for a compromise between system usability and privacy protection. Most fall in 2 teams. One approach is to switch information in a way in order that a confidence of the sensitive association is reduced. Some techniques were analysis to estimate what quantity such perturbation impact the standard of the results. {a informational knowledge an information} also can be sampled suitably to be chosen in such how on several any reasoning from this data have an occasional degree of confidence.

3.2 Access management:

While early work on integration info with necessary and discretionary access management created break although like System R Authorization Model, it had been too rigid and fitted to closed and controlled environments. The analysis of those models still continued. Necessary access provided the next level of security. Some analysis articulated a plan of poly instantiation, or having multiple copies with totally different security levels of constant tuple in relation.

3.3 Encryption:

It was completed early that whichever access management the info contained the soul still had how accessing the underlying information by wanting directly within the filing system or underlying storage. However, for an extended time science capabilities needed an important price burden for info operations and were\'t enclosed in any implementations. With will increase in process speed supporting secret writing of hold on information became possible in early 2000. At constant time many cases of adversaries and white hat hackers showed however simple it had been to getting data from previous discarded company onerous drives. For info's supporting secret writing of data created an extra issue for database optimisation techniques, like classification.



Data Security Consolidation [2]

3.4 Attack Detection:

With attackers making an attempt to reduce impact on the target system researches had to tackle a tangle of detective work a compromise. A aspect channel attack detection analysis is in progress and lots of intrusion detection merchandise have enclosed info modules. Data-centric approach relies on the key observation that question syntax alone may be a poor someone of user intent, that is far higher rendered by what\'s accessed. We tend to gift a feature-extraction technique to model users' access patterns.

IV. CONCLUSION

Databases are a unit a favorite target for attackers thanks to their information. There are units many ways within which a info may be compromised. There are a unit varied styles of attacks and threats from that a info ought to be protected. Solutions to most of the threats mentioned higher than are found, though some solutions area unit sensible whereas some area unit solely temporary. the assorted threats to the info area unit mentioned during this paper. it\'s vital to additionally note that several issues with securing information hold on within the info isn\'t as a result of the shortage of analysis however lacking security in implementation of the info product or associate degree application front ending the info. The shift from full trust to partial trust was driven partly by natural tendency to not give full trust to anyone single individual supported twin management principle however additionally as a result of the lack of the users to stay their own computer computers secure and info frontend not having the ability to sight malicious attacks like SQL injections.

REFERENCES

[1]: Database Security: Threats and Challenges by **Shelly Rohilla and Pradeep Kumar Mittal** Department of Computer Science & Applications Kurukshetra University, India Kurukshetra University, India

[2] : Database Security: A Historical Perspective "How the database security controls adapted to threats over the last 30 years" by UNIVERSITY OF MINNESOTA.

[3]: A Data-Centric Approach to Insider Attack Detection in Database Systems by Sunu Mathew, Michalis Petropoulos , Hung Q. Ngo , Shambhu Upadhyaya .