Indonesian Journal of Electrical Engineering and Computer Science
Vol. 1, No. 2, February 2016, pp. 406 ~ 410
DOI: 10.11591/ijeecs.v1.i2.pp406-410

Information Base Security Threats and Challenges' in Information Forensic: A Survey

Dilip Kumar Barai*, G. Sridevi, Syed umar, MSR Prasad
Dept. of CSE, KL University, Vaddeswaram, Guntur, India
*Corresponding author, email: dilipkumarb7@gmail.com

Abstract

Generally to store the information or Information of any organization then they will be maintain Information base to manage that Information base we use some management techniques like Information base management systems so called DBMS. In this paper we introduced Relational DBMS which is a collection of applications that can store various information which can be easily retrieve, manipulate and storage of Information. So in this we are concentrating on forensic analysis and Information base of it which is very sensitive Information. In this paper we are analyzing and surveying of forensic Information based using various methodologies with different tools and algorithms for investigations, through which we got what are the challenges are facing in the forensic Information bases since the years.

Keywords*: DBMS, RDBMS, forensic Information tools.*

1. Introduction

The main concept in this paper is how the security is maintained to the Information base which is used by the forensic department, if any misusage of will occur then, judgment will not be given to the accused people who did crime. There are more number of independent risks is there for the confidential Information stored in the Information base. So some issues like identity theft, audit failures etc., will happens. These will happen due to some reasons like 1) Financial constraints 2) Lack of threats understanding, 3) Interdepartmental cooperation is less, 4) No connection between the IT operations and executive programs, 5) Lack of security to the Information base processes and procedures etc. In the forensic department victim`s information and related Information will be stored, if any misusage occurred then there will be lack of evidence which will support them to convict. To avoid such attacks the Relational DBMS will play a major role to be aware from such attacks. So in this paper we are analyzing some difficult attacks which cannot be detected easily and new approaches are introduced how we can capture the evidence and can be produces at the jurisdiction.

2. Interlope and Forensic Aspects of a Information Base

Many mechanism has been implemented by the Information base server provides to authenticate & authorize user information. Those standard approaches regulated and supported by the Government. And also require some federal regulations [1] which will secure the systems from various hackers in which forensic will maintain the Information like medical information of the victims etc. So that Information has to save as very confidential in relational DBMS. So the forensic department should maintain the Information as secure whether any changes are made any other or not we have to check these once [2] interlope of any Information base by an authorized or unauthorized user can be easily detected by some algorithms like tilted bitmap forensic analysis.

For seeking the aspects of forensic dept. Information base Martin S. Oliver [2] considered some main points which consists of external, conceptual, internal approach for forensic Examination. So the following things have to be considered while the forensic investigation is going on.

Received August 11, 2015; Revised November 24, 2015; Accepted December 15, 2015

a) Initially check difference with the Information & conceptual layer. The Information layer may be the target of an attack by destructing or making any subtle changes in the Information dictionary.

b) The Information dictionary also contains information that may be of forensic interest itself. The external technique defines the Information to be provided to a specific user.

c) At the time of forensic investigation, the various views for various users generated by different schemes may be appropriate. The number of such external schemas only depends on the considered Information base.

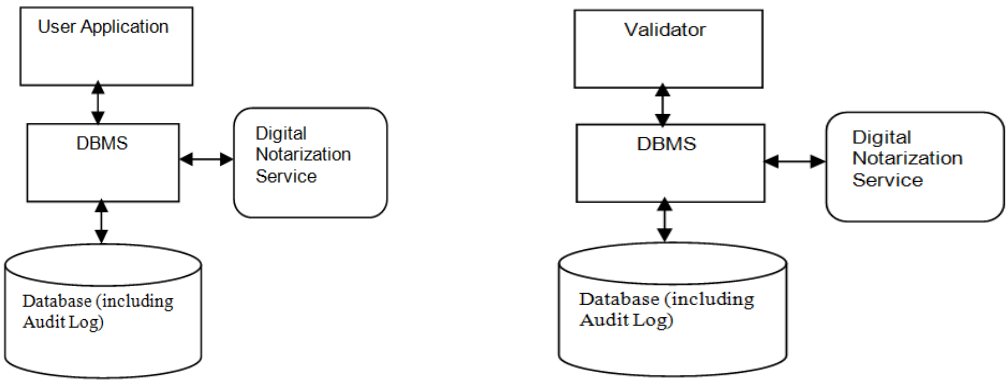
d) The OS management of the files used for the physical layer is also to be considered. Thus Martin S. Olivier considers the original ANSI/SPARC architecture (SIGMOD Record, 1982) which specified 42 interfaces between various components to explore Information base Forensics.

1) The level of logging should have enough information for investigation.
2) Restoration of information destroyed partially and the only partially recovered is undergone a forensic capture process.
3) Combination of both detailed logs and Mental formation may leads to determine who was authorized to perform certain action and use that as the basis for attribution.

3. Interpolation Detection Approaches

3.1. Cryptography Based Forensic Information Base Algorithms

A new improvised version of cryptographically strong one way hash functions which can prevent the hacker which cannot disturb the information in the Information base [3]. A module called notarize willed will be used which will send the hash value as a digital document in which it performs the notarization functions through this we will get the notary id. The notary id and along with the hash functional values will be stored in the smaller Information base [4]. Obtaining of notary is shown in the below Figure 1.



(a) Normal Operation (b) Audit log validation

Figure 1. Obtaining of notary id through the normal and audit operations

In a different physical location from the secured Information base a secure master Information base will be existed and will be under audit. Validity of the master Information base should be checked; the valuator will rescans the Information in the Information base hashes the scanned Information and sends the new hash value with the previous id which will be performance by the notarization service. By this notary id the it will check the previous hash values and new values are same or not, if not then the Information base will be compromised, Some algorithms has been implemented [1-3] when any tampered occurred to the Information or not will be checked.

3.2. Detection of Tampered Forensic of the Audit Logging

The detection and localization [5] of tampered forensic audit logging in the SQL server is said by Amit Basu. In this he explained that creation of interwoven chain of hash values with the help of detection and determination of audit table whether any changes did or not in it. If any information is inserted in the audit log it will be remain intact. So the Information base in the audit log will be protected, authenticate through the SQL server. So the tamper detection logic can be applied to the audit trail Information base which is having of two independent tables, they are Audit table and Audit user these are locate in the same application only. In this two special columns are there which will protect the audit log table called HReserved & VReserved which are shown in the below Figure 2.

1) In the HReserved the row hash values will be stored

2) In the VReserved the column hash values will be stored and it also contains hash value based on the HReserved values of the current row and the last two rows.

This method has various advantages it also suffers with some limitations like non-cryptographically strong hash functions and detection of forensic algorithm.

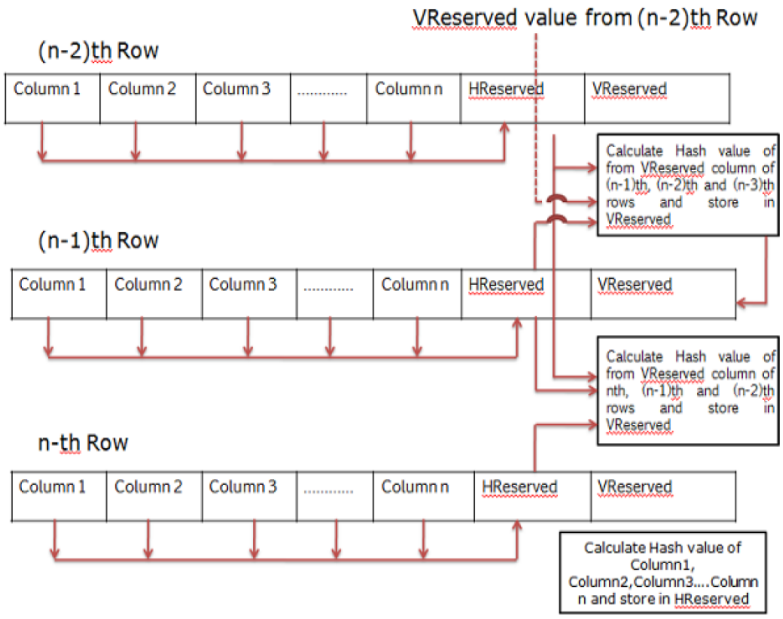


Figure 2. Detection and protection of audit log

3.3. Investigation and Artifacts of Information Base

How to collect the Information base artifacts which are more relevant in the Information base investigation, analyze them and find out the intrusion in the Information base and retracing of it with in the server will be clearly explained by Kevvie Fowler [6, 7]. Various SQL server artifacts are classified in two types. They are:

1) Resident Artifacts
2) Non Resident Artifacts

The Resident Artifacts are resides in the files and memory locations of the reserved locations of the SQL server. The Non Resident Artifacts are resides with in files but not explicitly reserved for the SQL reuse. The below Figure 3 shows the key artifacts

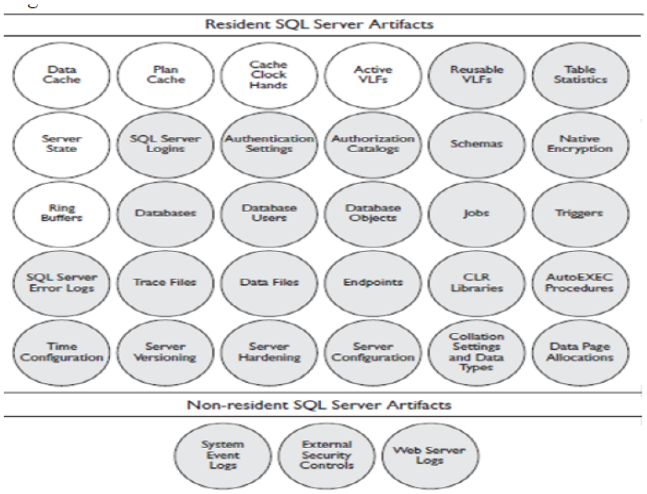


Figure 3. The SQL Artifacts

Each of the artifacts are explained in the below figure which is compressed of five types to which how they will benefit an investigation. Each artifacts will have its own way. The below table shows the categories of SQL [8] artifacts and it primary objective with in the investigation.

Table 1. Artifacts differentiation and its explanation

Artifact Category	Description
Activity reconstruction	Artifacts used to identify past and active database activity, such as created and modified database objects and executed SQL Server statements. Additionally, information on internal SQL Server operations, such as memory pressure conditions, can be identified.
Data recovery	Although activity reconstruction can identify the statements used to delete table data and objects in the database, data recovery artifacts will help you actually recover the deleted data.
Authentication and authorization	Artifacts used to identify failed and successful database login attempts and determine the level of access authenticated users have within the database. Analysis of these artifacts can reduce the list of possible suspects during an investigation.
Configuration and versioning	Artifacts used to identify enabled database features, the language of the characters stored within the database, and the actual format used by SQL Server in the storage of on-disk data. Analyzing these artifacts will provide mandatory information needed in almost every SQL Server investigation. Configuration and versioning artifacts can be used to identify the version of SQL Server running on a victim system. They will allow you to determine the appropriate version-specific statements to run during an investigation.
Not directly analyzed	Artifacts that are not specifically analyzed but used to aid in the analysis of other SQL Server artifacts.

4. Conclusion

In this paper we clearly explained how the Information base security should be maintain using some algorithms. Especially in the forensic department, the security for the server and Information base should be very high, misusage of information of victims medical information may lead to escape of accused from the jurisdiction. Different interpolation techniques are used for if any Information is encrypted or not and various approaches are discussed in this paper.

References

[1] KE Pavlou, RT Snodgrass. The Tiled Bitmap Forensic Analysis Algorithm. *IEEE Transactions on Knowledge and Information Engineering*. 2010; 22(4): 590-601.
[2] Martin S Olivier. On misinformation context in Information base Forensics. *Digital Investigation Volume.* 2009; 5(3-4): 115-123.

[3] Kyriacos Pavlou, Richard T Snodgrass. *Forensic Analysis of Information base Tampering*. International Conference on Management of Information, Proceedings of the ACM SIGMOD International Conference on Management of Information, SESSION: Authentication. 2006: 109-120.
[4] M Malmgren. An Infrastructure for Information base Tamper Detection and Forensic Analysis. Honors thesis. Univ. of Arizona. 2009.
[5] Article by A. Basu. Forensic Tamper Detection in SQL Server. 2006. http://www.sqlsecurity.com/images/tamper/tamperdetection.html
[6] SQL Server Forensic Analysis by Kevvie Fowler SQL Server Forensic Analysis, ISBN: 9780321533203.
[7] http://www.applicationforensics.com/research/microsoft/sql-server/sql-2000-2005-2008
[8] Paul M Wright. *Oracle Information base Forensics using LogMiner*. Conference, SANS Institute. 2005.