Detection of Attacks over Databases using Hashing Technique

Sushama R. Borhade[1], Sandip A. Kahate[2]

[1] ME Student Department of computer Engineering, SPCOE, Maharashtra,India.
[2] Assistant Professor Department of computer Engineering, SPCOE, Maharashtra, India

ABSTRACT

Now a days there is a increase in internet popularity which results in widely spreading the application of databases.So attackers creats the major problems with database to steal the data.And these Attackers decreases the truthfulness of database by modifying the data stored in the database. Attackers can easily copy ,download, or delete the database content .Now a days Backdoor attacks kept on increasing. It provide a camouflaged point of entry for hackers also offer various strategies for attack.So it is very important to avoid sush types of attacks because databases contains very confidential information about businesses or organizations.If this sensitive data gained by attacker then the organization may be collapse. In this paper we have tried to implement intrusion detection system to protect the database systems with the use of hash map .Hashing technique perfoms faster than other techniques and results in high performance and high efficiency in detecting the database attacks.

Keyword:- *Backdoor attacks,Intrusion,Intrusion Detection System,databases.Hash Map.*

1. INTRODUCTION

Attack is a potential for the occurrence of a harmful event against a target in the network[1].Basically attack is categorized into Passive attacks and Active attacks[2].In passive type of attack there is no any change in data on the targeted system.Its only about to make access the information of target.Attacker take access to the target through port scan.Sometimes these attack accesses the information to perform the future attack.Network Analysis ,Eavesdropping[3], Traffic Analysis etc.. are the examples of passive attack.And an active attack is one where the hacker modifies network packets while they are in transit, or sends forged network packets. During this, the intruder introduce data into the system as well as potentially change data within the system. They makes the unauthorized access to modify programs , escalating privileges ,causing a denial of service[4], accessing other systems. They affect the authentication ,integrity,and availability attributes of network security[5].

Day by day hackers are stepping towards the organization’s database server which is the heart of organizations that stores confidential business data ,customer records etc. Without having much knowledge of database, hackers can easily exploit the vulnerabilities to steal the private or sensetive data within it and to keep the security of these database systems,data,program or functions within them has become more critical because it takes the opened wide access through the networks.

1.1 Database Attacks

Database security can be violated by threats either by physically or logically. Physical threats means stealing of important data by hackers, revelation of passwords, demolition of storage devices and Logical threats mostly uses the vulnerabilities inside the software and with the help of these Vulnerabilities[12] hackers modifies the data ,reveal the Passwords, denial of service.Database attacks [6] are of different types they are as follows:

Insiders Threat: In this type of attack intruder pretends as a authorized person and sends the messages supposedly from legitimate users[11] .

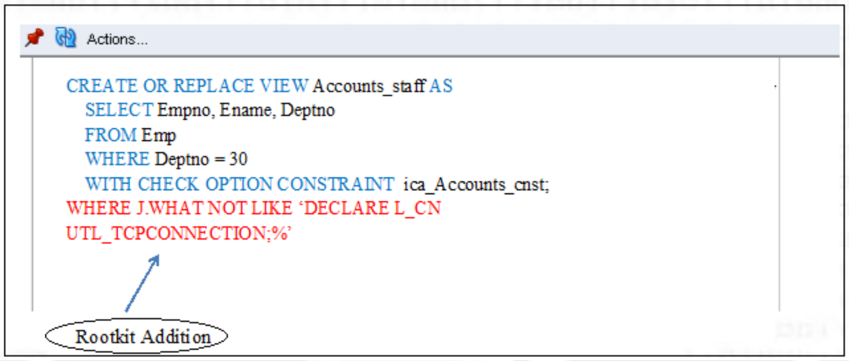
Trojan Horse:In this type of attack trojens[7] are deleiverd through CD,email, IM, pen drive, p2p,DVD ,etc.and Once it is executed attacker get database servers and login information to Connect to database servers then steal the data.By gaining this access attacker search the next target by checking at linked servers/databases, connections. And get encrypted data back by email, HTTPS, covert channel,etc.

SQL Attacks: In this attack attacker takes advantage of stored procedures and vulnerabilities in front-end web applications and sends unauthorize queries, often with elevated privileges[8].

Example:

Stealing data using a rootkit and backdoor:

After compromising the Oracle Database an attacker can install a backdoor to enable him/her to executequeries on the Database and get the responses back. A rootkit can be used to hide the backdoor from the DBA. To open a connection to the attacker's machine he/she Uses built-in network functionality and then reads the connection to execute the commands .this can be scheduled to run periodically so if the connection is failed due to some reasons, the attacker keep access by connecting at a later time.The backdoor can be reconfigured by the attacker using the backdoor itself.Following figure shows the rootkit addition in the database query.



```
CREATE OR REPLACE VIEW Accounts_staff AS
   SELECT Empno, Ename, Deptno
   FROM Emp
   WHERE Deptno = 30
   WITH CHECK OPTION CONSTRAINT  ica_Accounts_cnst;
WHERE J.WHAT NOT LIKE 'DECLARE L_CN
UTL_TCPCONNECTION;%'
```

Fig -1:Rootkit addition

2. . PROPOSED WORK

In the proposed work Intrusion Detection system is developed which sets the alerts to get the notifications when errors occurred on sensitive Database Servers depending on available functionality[10].

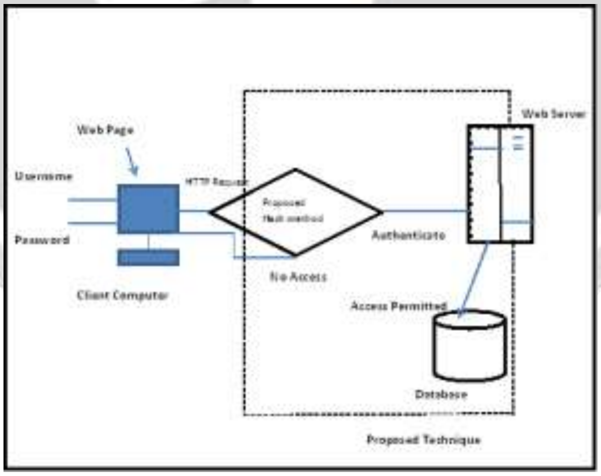


Fig 2: Proposed Technique

With the help of intrusion detection system based on hashing ,the attacker cannot bypass the process of authentication . The advantage of the this technique is that the attackers are unknow n about the hash values of confidential data i.e. user name and password. So,attack can be prevented with taking appropriate decision by security experts. At the backend ,Hash values are generated at the runtime so attackers are unable to calculate these values at runtime as it is dynamic.

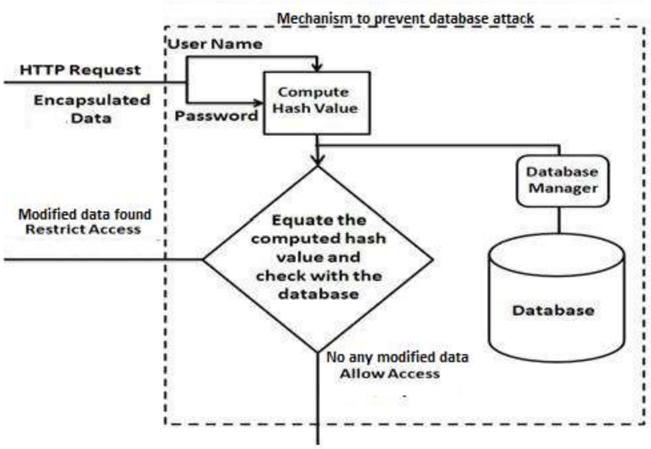

Mechanism to prevent database attack
User Name
HTTP Request
Encapsulated Data
Password
Compute Hash Value
Database Manager
Modified data found Restrict Access
Equate the computed hash value and check with the database
Database
No any modified data Allow Access

Fig -3: Mechanism to prevent attack

Specifically, the hash function is used to map the search key to an index; the index gives the place in the hash table where the corresponding record should be stored. Hash tables, in turn, are used to implement associative arrays and dynamic sets. Typically, the domain of a hash function (the set of possible keys) is larger than its range (the number of different table indices), and so it will map several different keys to the same index. Therefore, each slot of a hash table is associated with (implicitly or explicitly) a set of records, rather than a single record. For this reason, each slot of a hash table is often called a bucket, and hash values are also called bucket indices. Finding duplicate records.

3. WORKING METHODOLOGY

HashMap[9] is an array of Entry objects:
Consider HashMap as an array of objects.

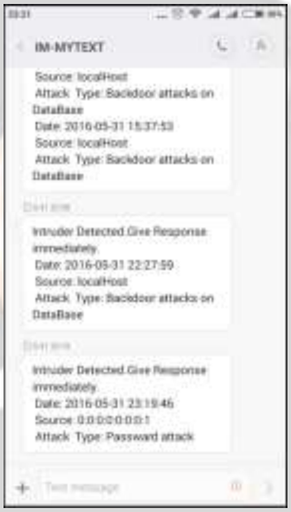
```
1 .class Entry <K,V>  implements  Map.Entry<K,V>
     {
        final K key;
        V value;
        Entry<K,V>  next;
        final int hash; ...
       }
2. Add a new key-value pair :
      (a)Calculate  hashcode for the key
      (b)Calculate  position as
          (hash %(arrayLength-1))
3. Creating  a HashMap :
      (a) put(K key, V value)
             {
              if (key == null)
              return putForNullKey(value);
      (b)    int hash= hash(key.hashCode());
              int i = indexFor(hash, table.length);
      (c)    addEntry(hash, key, value, i);
              return null;
             }
```

4 . to look up x in the map,calculate x.hashCode()
pick the appropriate bucket then iterate through
the bucket's list and pick the entry e where e.key
equals x.
then it returns e.value as given below

```
 List <List<Entry>>  buckets;
          Object get(Object key)
            {
              List<List<Entry>bucke  = buckets.get(key.hashCode()%buckets.size());
  (a)   for (Entry  entry : bucket)
            {
               if (Object.equals(key,  entry.key)
               return entry.value;
              }
            }
```

4. RESULTS

This technology helps in much extent to detect the database attacks with generating alerts over the mobile network.Following figure shows the notification of attack detected by system to take the appropriate action against the attack.



IM-MYTEXT

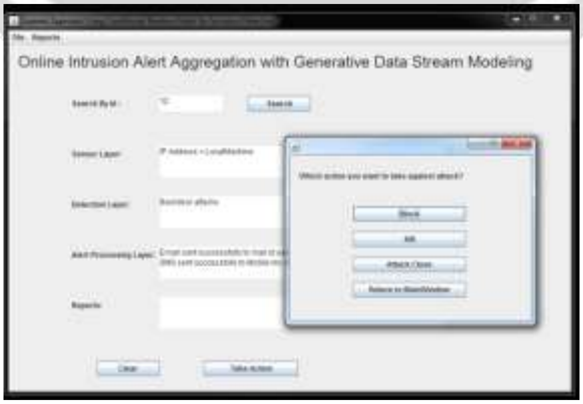
Source: localHost
Attack Type: Backdoor attacks on DataBase
Date: 2016-05-31 15:37:53
Source: localHost
Attack Type: Backdoor attacks on DataBase

Intruder Detected.Give Response immediately.
Date: 2016-05-31 22:27:59
Source: localHost
Attack Type: Backdoor attacks on DataBase

Intruder Detected.Give Response immediately.
Date: 2016-05-31 23:19:46
Source: 0:0:0:0:0:0:0:1
Attack Type: Password attack

Fig - 4: Alert of attack.

After getting notification of attack ,admin check out the behavior of attack in terms of attack type,its source IP address and according to behavior admin take the appropriate action like killing the process ,blocking the IP address or only close the attack with return to home page.



Online Intrusion Alert Aggregation with Generative Data Stream Modeling

Search By Id :
Sensor Layer: IP Address = LocalMachine
Detection Layer: Backdoor attacks
Alert Processing Layer:
Reports:

Which action you want to take against attack?

Fig -5 :Backdoor attack

5.CONCLUSION

In the today's IT world everyone wants to keep their confidential data as secure but many of the sources leads to hack the ones confidential information.So taking this under consideration proposed system works to protect the confidentiality, availability and the integrity constraints of the security . This uses the efficient algorithm of hashing technique which works on hashmap.This results in high performance and efficient technology when compared to existing techniques.

6.ACKNOWLEDGMENT

We would like to thanks all of the reserchers of the IEEE transactions and International Journals who made available their articles over the internet which helps us in great extent to implement our work.

7. REFERENCES

[1] Jatinder Teji, Rimmy Chuchra, Sonam mahajan, Manpreet Kaur Gill, Manju Dandi, "Detection and Prevention of Passive Attacksin Network Security", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013, ISSN: 2319-5967.

[2] Xiang-Yang Li, "Cryptography and Network Security", CS595.

[3] Markus G. Kuhn ,"Eavesdropping attacks on computer displays", Computer Laboratory, University of Cambridge,2006.

[4] Akash Mittal, Prof. Ajit Kumar Shrivastava,Dr. Manish Manoria," A Review of DDOS Attack and its Countermeasures in TCP Based Networks", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.

[5] Bhavya Daya ,"Network Security: History, Importance, and Future",University of Florida Department of Electri cal and Computer Engineering .

[6] K.A.Varunkumar, M.Prabakaran,Ajay Kaurav, S.Sibi Chakkaravarthy",Various Databas Attacks and its Prevention Techniques" International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 11 - Mar 2014.

[7] Hector J. Garcia, Jr., Texas A&M University-Kingsville, Dr. Ralph Reilly," TROJAN HORSES: THEY DECEIVE, THEY INVADE, THEY DESTROY", University of Hartford, IACIS 2003.

[8] Jai Puneet Singh," Analysis of SQL Injection Detection Techniques", CIISE, Concordia University.

[9] Parveen Sadotra,"Hashing Technique - SQL Injection Attack Detection & Prevention", International Journal of Innovative Research in Computer and Communication Engineering(IJIRCCE), Vol. 3, Issue 5, May 2015.

[10] Anandarup Sarkar,SvenK¨ohler,Sean Riddle,Bertram Ludasche, Matt Bishop," Insider Attack Identification and Prevention Using a Declarative Approach", 2014 IEEE Security and Privacy Workshops.

[11] Hossein Jadidoleslamy,"weaknesses ,vulnerabilities and elusion strategies against intrusion detection systems",International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.4, August 2012.

[12] Mohammed Alhanjouri, Ayman M. Al Derawi," A New Method of Query over Encrypted Data in Database using Hash Map", International Journal of Computer Applications (0975 – 8887) Volume 41– No.4, March 2012.