Beyond intrusion detection: The next frontier in safeguarding corporate assets

Ron Bennatan
CTO, Guardium Inc.

NYOUG Tech Journal
Sept, 2004
Databases - “The Crown Jewels”

- Databases are rich in content and functionality
  - Critical, sensitive and high integrity data is moving from applications to RDBMSs
  - Concentrate data and, therefore, risk

- Web Applications provide a high volume portal for database intrusions
  - Recent surveys indicate rising losses from database attacks (e.g. Evans Data)

- Generally weak implementation of data access/usage controls
  - Application bugs, non-current patches, lack of visibility and adherence to best practices

- Regulatory compliance enforcement - legal / regulatory pressure to protect information is increasing (eg. GLB, HIPPA, SOX)
Database Threats Are Increasing

- Pressures to deliver cause more holes
- Web applications (a portal to the database) are open to potentially every hacker in the world
- Hacker chatter about databases is rising
- Hacker conventions and workshops are focusing more on databases
- Surveys of database managers (e.g. Evans Data) indicate rising losses from database attacks
- Increasing class action lawsuits around privacy breaches
• So..
  – Database security is really important – and coming to the forefront

• But..
  – Doesn’t a database have adequate security and audit capabilities?
Yes.. And No..

• Strategy/philosophy – defense-in-depth
• Databases have bugs
• Database security model is limited
  – Implicitly needs to trust the application – which really cannot be trusted
  – Based primarily of login name and user/role permissions
    • Not on programs, network info, ..
    • Cannot do baselining etc.
  – Dependent on its own configuration – cannot do introspection
• Auditing features exist but are sometimes hard to use
  – Taxes the CPU and IO
  – Not dynamic (will talk about it later)
  – Cannot support segregation of duties
• Application vulnerabilities become data access vulnerabilities
Example 1: App server conf files

<data-source name="ORCL"
  class="oracle.jdbc.pool.OracleConnectionPoolDataSourc" username="scott"
  password="tiger"
  url="jdbc:oracle:thin:@orclsrv"
  connection-driver="oracle.jdbc.driver.OracleDriver"
  location="jdbc/orcl" xa-location="jdbc/xa/orcl"
  ejb-location="jdbc/orcl"
  connection-retry-interval="5"
  max-connect-attempts="5"
  inactivity-timeout="900"
  max-connections="100"
  min-connections="50"
  wait-timeout="900"/>

<ias-resources>
  <resource>
    <jndi-name>jdbc/ORCL</jndi-name>
    <jdbc>
      <database>ORCL</database>
      <datasource>ORCL</datasource>
      <username>scott</username>
      <password>tiger</password>
      <driver-type>ORACLE_OCI</driver-type>
    </jdbc>
  </resource>
</ias-resources>

weblogic.jdbc.connectionPool.eng=
url=jdbc:weblogic:oracle,\ndriver=weblogic.jdbc.oci.Driver,\nloginDelaySecs=2,\ninitialCapacity=50,\ncapacityIncrement=10,\nmaxCapacity=100,\nprops=user=scott,password=tiger,server=ORCL
Example 2 – SQL Injection & modification

- SELECT username FROM users WHERE username='XYZ' AND password='ABC'
  - SELECT username FROM users WHERE username='XYZ' AND password='ABC' OR '1'='1'
  - SELECT username FROM users WHERE username='XYZ' AND password='ABC' UNION ALL SELECT object_name FROM user_objects WHERE ''=''`

- SELECT name,ssec FROM customers WHERE id='XYZ'
  - SELECT name,ssec FROM customers where id LIKE '%'

- SELECT name,ssec FROM customers WHERE id='1'
  - SELECT name,ssec FROM customers WHERE id='2'
  - SELECT name,ssec FROM customers WHERE id='3'
  - SELECT name,ssec FROM customers WHERE id='4'
  - ...
  -
Oracle Vulnerabilities

- [www.cert.org](http://www.cert.org)
Example 3: Double Whammy

- SELECT FROM_TZ(TIMESTAMP '2004-09-07 18:00:00', '5:00') FROM DUAL;

- SELECT FROM_TZ(TIMESTAMP '2004-09-07 18:00:00', 'well crafted long string @(*#&$%^@#$sdfnhjkhsdfkhjfdhgkh9283748') FROM DUAL;
Example 4: Auditing semantic gap

Most of our important, sensitive and private data is in the RDBMS. We MUST audit access to the database. We MUST audit usage of data. We MUST audit maintenance/control/admin usage. If we don’t, we will not be in COMPLIANCE.

Hey – audit the database!

OK – What do you need to audit?

Hmmm…

Well – audit all reads of data, all writes, all changes to the database, who did it, from where, when, how, …

?!?!?

Are you serious?

Example 4: Auditing semantic gap
What does the security world have to offer?

- **Firewalls**
  - TCP/IP access control
    
    TCP.INVITED_NODES=(<Client IP-ADDRESS 1>, <Client IP-ADDRESS 2>)
    TCP.EXCLUDED_NODES=(<Client IP-ADDRESS 3>, <Client IP-ADDRESS 4>)
    TCP.VALIDNODE_CHECKING=yes

    protocol.ora for Oracle 8i  sqlnet.ora for Oracle 9i

- **Intrusion Detection Systems (IDS)/Intrusion Prevention Systems**
  - Detect/prevent misuse of network or computer resources
    - Sensors and rules
    - Libraries of signatures
    - “Deep packet inspection”
IDS Success – or lack-of

Gartner declares IDS obsolete by 2005

By Michael S. Mimoso, SearchSecurity.com News Editor
12 Jun 2003 | SearchSecurity.com

The death knell for intrusion detection is getting louder. Tired of doing full-time monitoring and fending off alerts that 99 times out of 100 mean nothing, enterprises have been ready to shove these expensive network-monitoring products off the proverbial cliff.

Research firm Gartner Inc. provided another nudge Wednesday when it declared IDS will be obsolete by 2005.

Instead, Gartner recommends that businesses invest their security dollars on firewalls that block attacks, rather than alert administrators to them.
Problem in applying IDS and deep packet inspection to database security

- Payload inspection is not enough – full SQL parsing and full protocol analysis is needed

UPDATE TEST_SQL SET TEXT='SELECT * FROM USER_OBJECTS UNION SELECT * FROM USER_OBJECTS WHERE 1=1'
More importantly

- Any attack can take on an infinite number of ways – signatures are pretty much useless in a SQL environment
  - 1=1, 2=2, 1<2, ‘ron’ like ‘ron%’, string concatenation, build in functions, …

- Bottom line: generic IDS/IPS are not effective for database protection

- Function-focused vs. environment-focused
  - IDS/IPS try to provide a function for many environments
  - Database environment requires multiple security/audit functions
Key Success Factors

- Full understanding and fit with the database and the DBA environment
  - Continuous SQL-level inspection
  - Full coverage of database options
  - SQL and other – based policies, alerts, etc.
  - Non intrusive
  - Complex access environments
  - Complex rules and configurations

- Breadth of functionality for database security and auditing
  - Policy-based real-time alerting and prevention
    - Before-the-fact or after-the-fact
  - Data access monitoring
  - Assessments
  - Auditing
  - ... Error monitoring and alerting
  - Investigations and forensic analysis

- Quick implementation and ability to be utilized with limited skill sets
  - Non-intrusive; zero risk
  - Many tasks do not require DBA skills
    - Stop overloading the DBA
    - Segregation of duties – put your money where your mouth is
Three approaches to “non-intrusive” monitoring

- SGA Queries
- Packet inspection
- Redo-log analysis
Auditing

Use an existing report, assessment or privacy set to...

Define an audit process

Task Description
- Schema Changes
- This task has not been scheduled
- Modify Schedule...

Task Type
- Auditing Report
- Security Assessment
- Entity Audit Trail
- Priv...

Keep for a minimum of 0 days or 5 runs

Auditing Report
- DDL Distribution

Task Parameters

QUERY_FROM_DATE
- Enter Period From

QUERY_TO_DATE
- Enter Period To

GROUPING_SUB_TYPE
- Choose Grouping Type
- Choose A Group Type Or Sub-Type to Group By

Rule
- No roles have been assigned to this Task

# Policies

## Rule Definition

<table>
<thead>
<tr>
<th>Select</th>
<th>Sequence</th>
<th>Rule Description</th>
<th>Client Ip</th>
<th>Server Ip</th>
<th>Source Program</th>
<th>DB User Group</th>
<th>Application User</th>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>SA rule</td>
<td>128.1.1.1/255.255.255.0</td>
<td>125.125.1.1/255.255.0.0</td>
<td>DBA</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suggested Rule_01-27 17:06</td>
<td>192.168.2.0/255.255.255.0</td>
<td>192.160.0.0/255.255.0.0</td>
<td>CRM</td>
<td>ANY</td>
<td>ANY</td>
<td>Suggested Object</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suggested Rule_02-13 11:18</td>
<td>192.163.2.0/255.255.255.0</td>
<td>192.168.0.0/255.255.0.0</td>
<td>CRM</td>
<td>ANY</td>
<td>ANY</td>
<td>Orders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suggested Rule_02-13 11:23</td>
<td>192.163.2.0/255.255.255.0</td>
<td>192.168.0.0/255.255.0.0</td>
<td>CRM</td>
<td>ANY</td>
<td>ANY</td>
<td>Suggested Object</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suggested Rule_02-18 16:2966</td>
<td>ANY</td>
<td>ANY</td>
<td>dbo</td>
<td>ANY</td>
<td>SYSXLOGSING</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suggested Rule_02-18 16:332</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>INFORMATION_SCHEMA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BASELINE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alert ALL</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hidden</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
</tr>
</tbody>
</table>

**Policy Description:** CRM Production June 2003

**Rule minimum count:** 1

**Minimum number of occurrences:** 1