The STIG and Database Security

John Calandra
McCallie Associates
DoD Contractor
The Information Assurance Support Environment Web Site
Security Technical Implementation Guides (STIGs)
Finding A STIG
The STIG Viewer
  - Loading a STIG
  - Manual Checklist
  - Checklist Export
Security Posture
  - Reporting
  - Strategy
  - Framework
  - Filtering & Refactoring SQL code from STIG
Questions & Answers
The Information Assurance Support Environment Web Site

Security Technical Implementation Guides (STIGs)

The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

Questions or comments?
Please contact DISA STIG Customer Support Desk:
disa.stig_spt@nsl.mil
The Information Assurance Support Environment Web Site: Finding Your STIG
The Information Assurance Support Environment Web site: A–Z STIG List
The Information Assurance Support Environment Web site: Oracle STIGs

<table>
<thead>
<tr>
<th>Product Description</th>
<th>Date</th>
<th>Size</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 11g Database STIG - Version 8, Release 15</td>
<td>10/23/2015</td>
<td>705 KB</td>
<td>ZIP</td>
</tr>
<tr>
<td>Oracle 12c Database Release Memo</td>
<td>10/18/2015</td>
<td>71 KB</td>
<td>PDF</td>
</tr>
<tr>
<td>Oracle 12c Database STIG - Version 1, Release 1</td>
<td>10/18/2015</td>
<td>395 KB</td>
<td>ZIP</td>
</tr>
<tr>
<td>Oracle Exadata Integrated Lights Out Manager</td>
<td>3/31/2015</td>
<td>617 KB</td>
<td>PDF</td>
</tr>
<tr>
<td>Oracle Exadata Storage Server</td>
<td>3/31/2015</td>
<td>582 KB</td>
<td>PDF</td>
</tr>
<tr>
<td>Oracle Exadata Sun Data Center InfiniBand Switch 36</td>
<td>3/31/2015</td>
<td>602 KB</td>
<td>PDF</td>
</tr>
<tr>
<td>Oracle Exadata ZFS Storage Appliance</td>
<td>3/31/2015</td>
<td>613 KB</td>
<td>PDF</td>
</tr>
<tr>
<td>Oracle Linux 5 IAVM - Version 1, Release 9 *PKI</td>
<td>11/30/2015</td>
<td>191 KB</td>
<td>ZIP</td>
</tr>
<tr>
<td>Oracle Linux 5 Manual STIG - Version 1, Release 4</td>
<td>10/23/2015</td>
<td>471 KB</td>
<td>ZIP</td>
</tr>
<tr>
<td>Oracle Linux 5 Manual STIG Release Memo</td>
<td>7/16/2014</td>
<td>58 KB</td>
<td>PDF</td>
</tr>
<tr>
<td>Oracle Linux 6 IAVM - Version 1, Release 9 *PKI</td>
<td>11/30/2015</td>
<td>191 KB</td>
<td>ZIP</td>
</tr>
<tr>
<td>Oracle Linux 6 Manual STIG - Version 1, Release 4</td>
<td>10/23/2015</td>
<td>386 KB</td>
<td>ZIP</td>
</tr>
<tr>
<td>Oracle Linux 6 Manual STIG Release Memo</td>
<td>7/13/2014</td>
<td>41 KB</td>
<td>PDF</td>
</tr>
</tbody>
</table>
The STIG Viewer

The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD’s security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

Questions or comments?
Please contact DISA STIG Customer Support Desk:
disa.stig_spt@mail.mil
# The STIG Viewer

![IASE Information Assurance Support Environment Logo](image)

## STIG Viewer

*PKI = DoD PKI Certificate Required

### STIG Viewer

<table>
<thead>
<tr>
<th>Download</th>
<th>Date</th>
<th>Size</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>STIG Viewer Quick Reference Guide</td>
<td>2/29/2012</td>
<td>2,261 KB</td>
<td>PDF</td>
</tr>
<tr>
<td>STIG Viewer Version 2.1</td>
<td>12/16/2015</td>
<td>617 KB</td>
<td>JAR</td>
</tr>
</tbody>
</table>

### Stylesheets Sorted by STIG ID

<table>
<thead>
<tr>
<th>Download</th>
<th>Date</th>
<th>Size</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>STIG Sorted by STIG ID</td>
<td>3/30/2015</td>
<td>105 KB</td>
<td>XSL</td>
</tr>
<tr>
<td>STIG Sorted by STIG ID - FOUO *PKI</td>
<td>3/30/2015</td>
<td>105 KB</td>
<td>XSL</td>
</tr>
</tbody>
</table>

### Stylesheets Sorted by Vulnerability ID

<table>
<thead>
<tr>
<th>Download</th>
<th>Date</th>
<th>Size</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>STIG Sorted by Vulnerability ID</td>
<td>3/30/2015</td>
<td>102 KB</td>
<td>XSL</td>
</tr>
<tr>
<td>STIG Sorted by Vulnerability ID - FOUO *PKI</td>
<td>3/30/2015</td>
<td>105 KB</td>
<td>XSL</td>
</tr>
</tbody>
</table>
Rule Title: Audit trail data must be retained for at least one year.

STIG ID: 0121-IP-021100  Rule ID: SV-7589r1_rule  Vuln ID: V-61409
Severity: CAT II Class: Unclass

Discussion:
Without preservation, a complete discovery of an attack or suspicious activity may not be determined. DBMS audit data also contributes to the complete investigation of unauthorized activity and needs to be included in audit retention plans and procedures.

Documentable: No

Check Content:
Review and verify the implementation of an audit trail retention policy.
Verify that audit data is maintained for a minimum of one year.
If audit data is not maintained for a minimum of one year, this is a finding.

Fix Text:
Develop, document and implement an audit retention policy and procedures.
It is recommended that the most recent thirty days of audit logs remain available online.
After thirty days, the audit logs may be maintained off-line.

Online maintenance provides for a more timely capability and inclination to investigate suspicious activity.

CCX: CCI-000366
NIST SP 800-53 :: CM-6 b
NIST SP 800-53a :: CM-6.1 (iv)
NIST SP 800-53 Revision 4 :: CM-6 b
The STIG Viewer: Loading a STIG
The STIG Viewer: Manual Checklist
The STIG Viewer: Manual Checklist

Discussion:
The configuration option SQL92_SECURITY specifies whether table-level SELECT privileges are required to execute an update or delete that references table column values. If this option is disabled (set to FALSE), the UPDATE privilege can be used to determine values that should require SELECT privileges.

The SQL92_SECURITY setting of TRUE prevents the exploitation of user credentials with only DELETE or UPDATE privileges on a table from being able to derive column values in that table by performing a series of update/delete statements using a WHERE clause, and rolling back the change. In the following example, with SQL92_SECURITY set to FALSE, a user with only delete privilege on the scott.EMP table is able to derive that there is one employee with a salary greater than 3000. With SQL92_SECURITY set to TRUE, that user is prevented from attempting to derive a value.

SQL92_SECURITY = FALSE
SQL> delete from scott.EMP where sal > 3000;
1 row deleted
SQL> rollback;
Rollback complete

SQL92_SECURITY = TRUE
SQL> delete from scott.EMP where sal > 3000;
delete from scott.EMP where sal > 3000;
* ERROR at line 1: ORA-01031: insufficient privileges
The STIG Viewer: Manual Checklist


- File
- Import
- Export
- Options

<table>
<thead>
<tr>
<th>STIG ID</th>
<th>Rule</th>
<th>Severity</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>O121-BP-021100 - SRG-APP-000516</td>
<td>Oracle SQL92_SECURITY parameter must be set to TRUE.</td>
<td>Not a Finding</td>
<td>Unclass</td>
</tr>
<tr>
<td>O121-BP-021200 - SRG-APP-000516</td>
<td>Rule ID: SV-75919r1_rule Vuln ID: V-61429</td>
<td>Not a Finding</td>
<td>Unclass</td>
</tr>
<tr>
<td>O121-BP-021300 - SRG-APP-000516</td>
<td>STIG ID: SQL92_SECURITY</td>
<td>Not a Finding</td>
<td>Unclass</td>
</tr>
<tr>
<td>O121-BP-021400 - SRG-APP-000516</td>
<td>Description:</td>
<td>Not a Finding</td>
<td>Unclass</td>
</tr>
<tr>
<td>O121-BP-021500 - SRG-APP-000516</td>
<td>The configuration option SQL92_SECURITY specifies whether table-level privileges. If this option is disabled (set to FALSE), the update privileges.</td>
<td>Not a Finding</td>
<td>Unclass</td>
</tr>
<tr>
<td>O121-BP-021600 - SRG-APP-000516</td>
<td>The SQL92_SECURITY setting of TRUE prevents the exploitation of user privilege by performing a series of update/delete column values in that table.</td>
<td>Not a Finding</td>
<td>Unclass</td>
</tr>
<tr>
<td>O121-BP-021700 - SRG-APP-000516</td>
<td>The following example, with SQL92_SECURITY set to FALSE, a user with only employee with a salary greater than 3000. With SQL92_SECURITY set to TRUE.</td>
<td>Not a Finding</td>
<td>Unclass</td>
</tr>
</tbody>
</table>

```sql
SQL92_SECURITY = FALSE
SQL> delete from scott.emp where sal > 3000;
1 row deleted
SQL> rollback;
Rollback complete

SQL92_SECURITY = TRUE
```

Discussion:

The configuration option SQL92_SECURITY specifies whether table-level privileges. If this option is disabled (set to FALSE), the update privileges. The SQL92_SECURITY setting of TRUE prevents the exploitation of user privilege by performing a series of update/delete column values in that table. The following example, with SQL92_SECURITY set to FALSE, a user with only employee with a salary greater than 3000. With SQL92_SECURITY set to TRUE.
The configuration option SQL92_SECURITY specifies which column values. If this option is disabled (set privileged).

The SQL92_SECURITY setting of TRUE prevents the expression of column values in that table by performing a SELECT statement, with SQL92_SECURITY set to FALSE, on an employee with a salary greater than 3000. With SQL92_SECURITY = FALSE:

SQL> delete from scott.emp where sal > 3000;
1 row deleted
SQL> rollback;
Rollback complete
The STIG Viewer: Checklist Export

Rule Title: The Oracle SQL92_SECURITY parameter must be set to TRUE.

File...
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>V-61409</td>
<td>medium</td>
<td>O121-BP-021100</td>
<td>Audit trail data must be retained for at least one year.</td>
</tr>
<tr>
<td>2</td>
<td>V-61411</td>
<td>medium</td>
<td>O121-BP-021200</td>
<td>Access to default accounts used to support replication must be restricted to authorized DBA.</td>
</tr>
<tr>
<td>3</td>
<td>V-61413</td>
<td>medium</td>
<td>O121-BP-021300</td>
<td>Oracle instance names must not contain Oracle version numbers.</td>
</tr>
<tr>
<td>4</td>
<td>V-61415</td>
<td>medium</td>
<td>O121-BP-021400</td>
<td>Fixed user and public database links must be authorized for use.</td>
</tr>
<tr>
<td>5</td>
<td>V-61417</td>
<td>medium</td>
<td>O121-BP-021500</td>
<td>A minimum of two Oracle control files must be defined and configured to be stored on separate volumes.</td>
</tr>
<tr>
<td>6</td>
<td>V-61419</td>
<td>medium</td>
<td>O121-BP-021600</td>
<td>A minimum of two Oracle redo log groups/files must be defined and configured to be stored.</td>
</tr>
<tr>
<td>7</td>
<td>V-61421</td>
<td>medium</td>
<td>O121-BP-021700</td>
<td>The Oracle WITH GRANT OPTION privilege must not be granted to non-DBA or non-Applicat.</td>
</tr>
<tr>
<td>8</td>
<td>V-61423</td>
<td>medium</td>
<td>O121-BP-021800</td>
<td>Execute permission must be revoked from PUBLIC for restricted Oracle packages.</td>
</tr>
<tr>
<td>9</td>
<td>V-61425</td>
<td>high</td>
<td>O121-BP-021900</td>
<td>The Oracle REMOTE_OS_AUTHENT parameter must be set to FALSE.</td>
</tr>
<tr>
<td>10</td>
<td>V-61427</td>
<td>high</td>
<td>O121-BP-022000</td>
<td>The Oracle REMOTE_OS_ROLES parameter must be set to FALSE.</td>
</tr>
<tr>
<td>11</td>
<td>V-61429</td>
<td>medium</td>
<td>O121-BP-022100</td>
<td>The Oracle SQL92_SECURITY parameter must be set to TRUE.</td>
</tr>
<tr>
<td>12</td>
<td>V-61431</td>
<td>medium</td>
<td>O121-BP-022200</td>
<td>The Oracle REMOTE_LOGIN_PASSWORDFILE parameter must be set to EXCLUSIVE or NONE.</td>
</tr>
<tr>
<td>13</td>
<td>V-61433</td>
<td>medium</td>
<td>O121-BP-022300</td>
<td>System privileges granted using the WITH ADMIN OPTION must not be granted to unauthorized users.</td>
</tr>
<tr>
<td>14</td>
<td>V-61435</td>
<td>medium</td>
<td>O121-BP-022400</td>
<td>System Privileges must not be granted to PUBLIC.</td>
</tr>
<tr>
<td>15</td>
<td>V-61437</td>
<td>medium</td>
<td>O121-BP-022500</td>
<td>Oracle roles granted using the WITH ADMIN OPTION must not be granted to unauthorized users.</td>
</tr>
<tr>
<td>16</td>
<td>V-61439</td>
<td>medium</td>
<td>O121-BP-022600</td>
<td>Object permissions granted to PUBLIC must be restricted.</td>
</tr>
<tr>
<td>17</td>
<td>V-61441</td>
<td>high</td>
<td>O121-BP-022700</td>
<td>The Oracle Listener must be configured to require administration authentication.</td>
</tr>
<tr>
<td>18</td>
<td>V-61443</td>
<td>medium</td>
<td>O121-BP-022800</td>
<td>Application role permissions must not be assigned to the Oracle PUBLIC role.</td>
</tr>
<tr>
<td>19</td>
<td>V-61445</td>
<td>medium</td>
<td>O121-BP-022900</td>
<td>Oracle application administration roles must be disabled if not required and authorized.</td>
</tr>
<tr>
<td>20</td>
<td>V-61447</td>
<td>medium</td>
<td>O121-BP-023000</td>
<td>Connections by mid-tier web and application systems to the Oracle DBMS must be protected.</td>
</tr>
</tbody>
</table>
Security Posture

- John’s definition of Security Posture:
  
  A security posture is the means by which all events contrary to planned operation of a system are detected and thwarted.

- A [database] security posture includes detection of invalid
  - User events (logins, access)
  - Account events (creation, locked)
  - Configuration settings (permissions, settings)
  - Jobs (failures, long-running)
A security posture is not only detection/mitigation of threats – it is also ensures your database is set up and running properly!
Security Posture: Reporting

- Two types
  - Full-blown STIG reports
  - Monitoring reports

- Full-blown STIG reports
  - All items on STIG reported
  - Open items on report (findings) may be required to be placed on a POA&M (Plan of Action & Milestones)
  - POA&M typically required by Security/IA personnel

- Monitoring reports
  - Customized reports intended for internal use
  - Purpose is for maintenance of the security posture
  - Monitoring reports

- To be manageable, both types of reporting should be automated
Security Posture: Reporting

- Full-Blown STIG
  - All STIG items reported (coded + policy)
  - Non-STIG related items excluded
  - Item status
    - Coded checks: OPEN (finding) or Not A Finding
    - Policy checks: OPEN or CLOSED with explanation (one-liner)

- Monitoring
  - Reports contain only invalid items
  - Reports include non-STIG related items
  - Reports exclude policy items
  - Intent of report is to mitigate invalid items
Security Posture: Strategy

- **Goal:** Programming that automates detection/reporting of invalid events on a scheduled basis

- Two general types of invalid events
  - User-related events
  - Configuration settings

- Frequency of checks
  - Daily
  - Weekly
  - Monthly
  - Quarterly (full STIGs)
Steps

1. Review STIG – make list of “coded” checks vs. “policy” checks
   - Coded check: STIG supplies SQL – some items may need to be checked by OS commands only or SQL + OS commands
   - Policy check: No code, it is a one-time manual inspection but requires explanation

2. Determine items that need to be checked by automation but not in STIG – write code

3. Categorize coded checks by frequency (daily, weekly, monthly)
Security Posture: Strategy

User-Related Events

Configuration Settings

Daily Weekly Monthly
Security Posture: Strategy

- Steps
  1. Review STIG – make list of “coded” checks vs. “policy” checks
    - Coded check: STIG supplies SQL – some items may need to be checked by OS commands only or SQL + OS commands
    - Policy check: No code, it is a one-time manual inspection but requires explanation
  2. Determine items that need to be checked by automation but not in STIG – write code
  3. Categorize coded checks by frequency (daily, weekly, monthly)
Security Posture: Framework

1. STIG Script
2. Daily Monitoring
3. Weekly Monitoring

- SQL Scripts
- Output Files
- Evaluate output files, Format reports
- Daily Monitoring Report
- Weekly Monitoring Report
- Monthly Monitoring Report
- STIG Report
Security Posture: Framework

1. Start STIG script
2. Call SQL script
3. Generate output file
4. Evaluate output file
5. Format output/write to report

More checks? [Yes/No]

Report finished
Rule Title: System privileges granted using the WITH ADMIN OPTION must not be granted to unauthorized user accounts.

STIG ID: O121–BP–02230

Code (next slide)
Security Posture:
Filtering & Refactoring SQL code from STIG

- STIG ID: O121–BP–02230
- Check content code from STIG (code in dark grey is filter list):

  ```sql
  select grantee, privilege from dba_sys_privs
  where grantee not in ('SYS', 'SYSTEM', 'AQ_ADMINISTRATOR_ROLE', 'DBA', 'MDSYS', 'LBACSYS', 'SCHEDULER_ADMIN', 'WMSYS')
  and admin_option = 'YES'
  and grantee not in
  (select grantee from dba_role_privs where granted_role = 'DBA');
  ```
Issues with using SQL code from STIG as-is:
- Code should be refactored for readability and maintainability
- Something in SQL output is needed so that the output can be recognized as a finding
- Privileged accounts not in the filter list may show up in output
- Make SQL code from STIG into a reusable file
Security Posture:
Filtering & Refactoring SQL code from STIG

- STIG ID: O121–BP–02230
- There is a privileged account for DBA admins called ORA_ADMIN
- Refactored check content code from STIG:

  SELECT
    'ALERT:' as ALERT, 
  grantee, 
  privilege
FROM dba_sys_privs where grantee not in ( 
  'AQ_ADMINISTRATOR_ROLE', 
  'DBA', 
  'LBACSYS', 
  'MDSYS', 
  'ORA_ADMIN',< 
  'SCHEDULER_ADMIN', 
  'SYS', 
  'SYSTEM', 
  'SYSTEM', 
  'WMSYS')
AND admin_option = 'YES'
AND grantee not in ( 
  SELECT grantee from dba_role_privs 
  WHERE granted_role = 'DBA');

ALERT added to
SELECT as search item

Select, filter list refactored for
readability/maintainability

ORA_ADMIN
added to filter list

with_admin_option.sql
The STIG and Database Security

- Questions & Answers