Real World Database Auditing

Stephen Kost
Integrigy Corporation
Session # 602

Introduction

- **Stephen Kost**
  - Chief Technology Officer of Integrigy Corporation
  - 14 years experience with Oracle technology as database administrator, architect, and application administrator
  - Found more than 40 security bugs fixed in CPUs
- **Integrigy Corporation**
  - Dedicated to Oracle Security
  - Services – Oracle Security Assessments
  - Products – AppSentry and AppDefend

Agenda

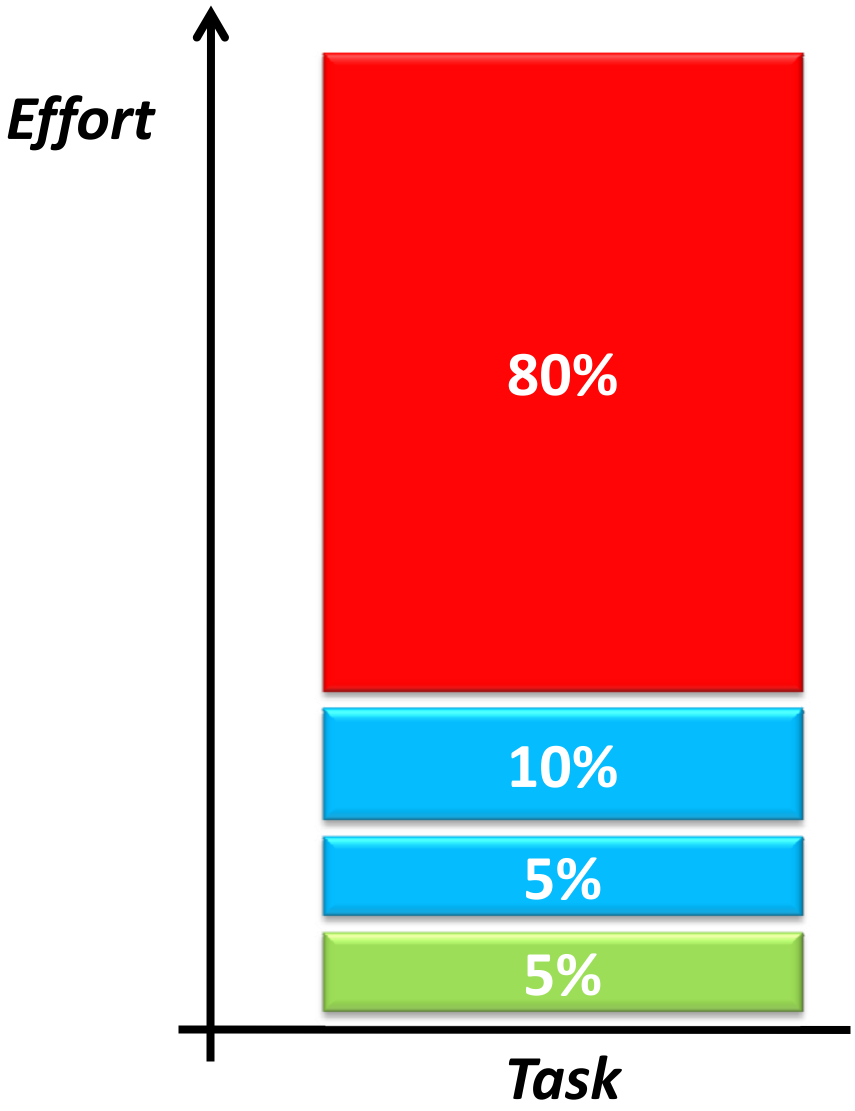
- Overview
- Managing
- Protecting
- Spoofing
- Third-party Tools

Some auditing is
always better than none …

Designed auditing is
always better than some auditing

“Reasonable Assurance”

that I can catch someone doing something ***bad***

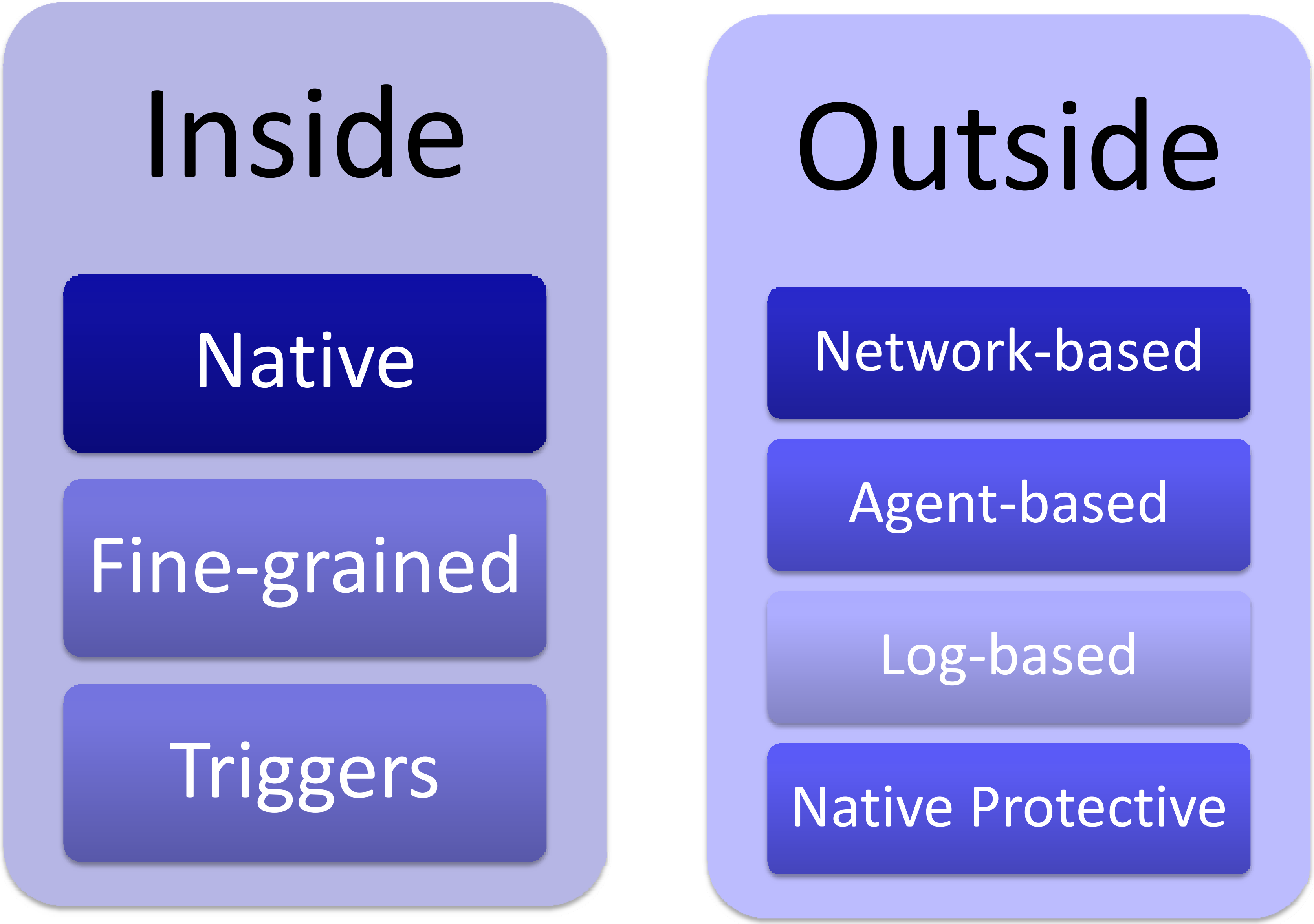


Monitoring,
Alerting,
Reporting,
Reviewing

Archiving & Purging

Designing

Enabling



Inside

- Native
- Fine-grained
- Triggers

Outside

- Network-based
- Agent-based
- Log-based
- Native Protective

ALWAYS* enable native auditing

AUDIT_TRAIL initialization parameter

```
os  db db_extended
 xml xml_extended
```

**No performance impact if just enabled*

Managing

Moving SYS.AUD$

Supported by Oracle? ***Recommended?***

Metalink Note ID 72460.1
Not Supported, but here's how

9.2.0.8 Admin Guide
Should not be moved

11.1 Security Guide
Consider moving it

Backups and Upgrades
Moving may cause problems

Why Move SYS.AUD$?

"If the audit trail becomes completely full and no more audit records can be inserted, audited statements cannot be successfully executed until the audit trail is purged. Warnings are returned to all users that issue audited statements."

- **Able to cause a denial of service if can fill-up the audit trail**

Introducing DBMS_AUDIT_MGMT

- 10.2.0.3, 10.2.0.4, 11.1.0.x support for moving AUD$ and FGA_LOG$ to new tablespace
  - Only currently available for most popular platforms
  - Granted to EXECUTE_CATALOG_ROLE
- See Audit Vault documentation for most detailed information
- See Metalink Note ID 731908.1

DBMS_AUDIT_MGMT

- **SET_AUDIT_TRAIL_LOCATION**
  – Move AUD$/FGA_LOG$ to a new tablespace

```
SQL> begin
  2   DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION(
  3   audit_trail_type =>
          DBMS_AUDIT_MGMT.AUDIT_TRAIL_DB_STD,
  4   audit_trail_location_value => 'AUDIT_TS');
  5   end;
  6   /
```

DBMS_AUDIT_MGMT

- **CLEAN_AUDIT_TRAIL**
  – Manually purge audit trail

```
SQL> begin DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
   2 AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_DB_AUD,
   3 USE_LAST_ARCH_TIMESTAMP => TRUE );
   4 end;
   5 /
```

DBMS_AUDIT_MGMT

- **Purge Jobs**
  - Schedule jobs to purge audit tables using INIT_CLEANUP, CREATE_PURGE_JOB, SET_PURGE_JOB_STATUS
- **Manage OS Auditing Files**
  - Can control size or age of OS level audit trail files

Protecting

Audit Trail Destination Options

Oracle Version	AUDIT_TRAIL	SYSDBA	FGA
8.0.x	OS/DB	-	-
8.1.x	OS/DB	-	-
9.0.x	OS/DB	-	DB
9.2.x	OS/DB	OS	DB
10.1.x	OS/DB	OS	DB
10.2.x	OS/DB/XML/ SYSLOG	OS/XML	DB/XML
11.1.x	OS/DB/XML/ SYSLOG	OS/XML	DB/XML

Audit Trail Destination – Database

- AUD$ and FGA_LOG$
  - Check privileges on these tables and any views such as DBA_AUDIT_* and DBA_FGA_AUDIT_TRAIL
  - Default privilege is DELETE for DELETE_CATALOG_ROLE
  - Database Vault can be used

Audit Trail Destination – OS

- Files must be owned by Oracle owner
  - Any Oracle process still can access the files, including UTL_FILE
- Always set AUDIT_FILE_DEST
  - Otherwise files go to $ORACLE_HOME/rdbms/audit
  - Check permissions on AUDIT_FILE_DEST
- Check privileges on V$XML_AUDIT_TRAIL

Audit Trail Destination – SYSLOG

- **AUDIT_SYSLOG_LEVEL=facility.priority**
  - Available in 10.2 and 11.1
  - Set AUDIT_TRAIL=OS
  - Audit trail and SYS audit trail written to standard Unix/Linux Syslog
  - Can only be modified by root and completely protected from DBA, except disabling auditing
  - Can be sent to external logging system
  - Does not include database SID

Spoofing

Session Value	V$SESSION View	SYS_CONTEXT Function	SYS.AUD$ DBA_AUDIT_*	FGA_LOG$ AUDIT_TRAIL	Audit Vault
DB User Name	✓	✓	✓	✓	✓
Schema Name	✓	✓			
OS User Name	✓	✓	✓	✓	✓
Machine	✓	✓	✓	✓	✓
Terminal	✓	✓	✓		✓
Program	✓				✓
IP Address		✓	✓		✓
Client Process ID	✓				
Module	✓	✓			
Action	✓	✓			
Client Info	✓	✓			✓
Client ID	✓	✓	✓	✓	✓

Auditing Session Data

Database User Name	OS User Name	Schema Name
IP Address	Machine/ User host	Terminal
Program	Client Process ID	Module
Action	Client Info	Client ID

Auditing Session Data – Spoofable

Database User Name	~~OS User Name~~	~~Schema Name~~
IP Address	~~Machine/ User host~~	~~Terminal~~
~~Program~~	~~Client Process ID~~	~~Module~~
~~Action~~	~~Client Info~~	~~Client ID~~

Spoofing Audit Session Data

- Easy to spoof client supplied session values using a custom program
  - Java/JDBC is easiest, but possible using any Oracle client
- Only timestamp, IP address, DB user name, and SQL are reliable
  - Look at V$SESSION – often granted to PUBLIC

Java Code to Spoof Session Values

```
java.util.Properties info = new java.util.Properties();

info.put("v$session.osuser", "dummy-osuser");
info.put("v$session.terminal", "dummy-terminal");
info.put("v$session.machine", "dummy-machine");
info.put("v$session.program", "dummy-program");
info.put("v$session.process", "123456");
info.put("v$session.module", "dummy-module");
conn.setClientIdentifier("dummy-clientidentifier");

java.sql.Connection conn =
        (new oracle.jdbc.OracleDriver()).connect(url,info);
```

Third-party Auditing Solutions

Third Party Auditing Solutions

- Define your **STRATEGY** first
  - Database security and auditing strategy is critical to successful implementation
  - Define responsibilities for DB security and auditing – difficult in most organizations
  - The strategy will drive the requirements

Third Party Auditing Solutions

- **There are fundamental differences among the vendors**
  - **Database activity capture vs. intrusion detection**
  - Data Capture Techniques = network, agent, log, native
  - Architecture = appliance vs. software
  - Bells and whistles = connection pooling, blocking, assessment, etc.

Application Security *AppRadar*	**Embarcadero** *DSAuditor*	**Guardium** *SQLGuard*
Imperva *DB Monitoring*	**Fortinet*** *IPLocks*	**Lumignet** *Audit DB*
Nitro Security *NitroGuard DBM*	**Secerno** *DataWall*	**Sentrigo** *Hedgehog*
Symantec *Database Security*	**Tizor*** *Mantra*	**Oracle** *Audit Vault*

My Other Sessions

IOUG

Critical Patch Updates: Insight and Understanding – Database

Wednesday, 8:30am to 9:30am

Room 222B

OAUG

Critical Patch Updates Unwrapped – Oracle E-Business Suite

Wednesday, 9:45am to 9:30am

Room 304G

Questions?

Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

e-mail: skost@integrigy.com
blog: integrigy.com/oracle-security-blog

For information on -

- Oracle Database Security
- Oracle E-Business Suite Security
- Oracle Critical Patch Updates
- Oracle Security Blog

www.integrigy.com