Data Security in ERP

and Other Large Business Systems

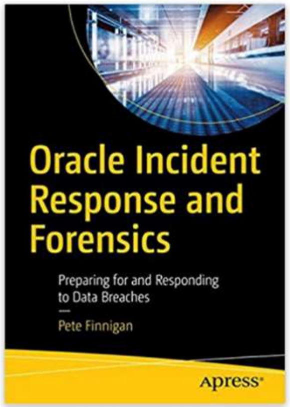
Legal Notice

Data Security in ERP and Other Large Business Systems

Published by
PeteFinnigan.com Limited
Tower Court
3 Oakdale Road
York
England, YO30 4XL

Limit of Liability / Disclaimer of warranty. This information contained in this course and this material is distributed on an "as-is" basis without warranty. Whilst every precaution has been taken in the preparation of this material, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions or guidance contained within this course.

TradeMarks. Many of the designations used by manufacturers and resellers to distinguish their products are claimed as trademarks. Linux is a trademark of Linus Torvalds, Oracle is a trademark of Oracle Corporation. All other trademarks are the property of their respective owners. All other product names or services identified throughout the course material are used in an editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this course.


Oracle Incident Response and Forensics
Preparing for and Responding to Data Breaches
Pete Finnigan
Apress

Pete Finnigan – Background, Who Am I?

- Oracle Security specialist and researcher
- CEO and founder of PeteFinnigan.com Limited in February 2003
- Writer of the longest running Oracle security blog
- Author of the Oracle Security step-by-step guide and "Oracle Expert Practices", "Oracle Incident Response and Forensics" books
- Oracle ACE for security
- Member of the OakTable
- Speaker at various conferences
  - UKOUG, PSOUG, BlackHat, more..
- Published many times, see
  - http://www.petefinnigan.com for links
- Influenced industry standards
  - And governments

Agenda

- Introduction
- Traditional ERP security
- The GAP in ERP security
- Some examples
- How to secure data in an ERP environment

Section

Introduction

Where Are We Going Today?

- My focus is database security
- I regularly audit databases that support ERP (and other big business applications)
- Usually I see a complete lack of any semblance of security at the data layer when its supporting ERP
- This discussion is not specific to one ERP/Big application
- I want to broaden the discussion beyond ERP security and focus on the data layer

Section

Traditional ERP Security

ERP Security

- At a high level ERP security if often discussed / complied with at …:
  - Separation of duties (SOD)
  - Conflict of interest (COI)
  - ERP level security settings – forms / menus / blocks / field level
- Fraud / Limits / Business Level
- Compliance with higher level rules / stds

ERP Layers

- ERPs are not just an ERP
- There are many layers underneath of
  - Application screens
  - Application and web servers
  - Reporting servers
  - Databases
  - Operating systems
- People normally access ERPs at the ERP level not lower level
- Some users often are allowed lower level access
  - Customisations / Excel / Reports / SQL*Developer / TOAD…

Where is ERP Security?

- The settings, configuration and other mechanisms can be in many places in an ERP
- Settings for the high level application security can be in the database for ephemeral settings and tech settings or in binaries, configuration files
- Often ERP have technical settings for the ERP in the database, servers, and configurations
- The supporting servers **can be** secured
- The supporting databases **can be** secured
- Complex layers where the DB plays two roles
  - Stores business data and config of the application

Black Box

- The database if often treated as a black box
- This is wrong
- Data thieves do not take this approach
- Attackers don’t care
  - About ERP settings or database settings
  - Or OS settings or database settings
- If an attacker can access the database or OS directly they will and they will steal data

ERP Data Level Security Is Often Missing

- Often there are no database level protections on data
- Some may use TDE – but without DV or similar to prevent SQL access this protects only the files
- Some may use VPD or Database Vault
- Some use masking, redaction, etc
- BUT by default, often data is **not** protected at the table level

The Data Attacker

- The Attacker is not a kid in his bedroom but most likely someone who works for you directly or via a 3rd party
- Hacking is not always hacking but excessive rights and misuse and authority failures
- I want to explore this loophole between data and ERP further

Section

The GAP

ERP Security – The Problem Space

- ERP systems such as JDE, EBS, Siebel, SAP and more are often focused at a business function level
- Security is at the ERP level and
  - Driven on fraud, money, SOD and COI
  - Often sites ignore the server and database and network levels – specifically in terms of the audit conducted
- The bridge between ERP and database and server is not considered seriously enough
  - That does not mean companies do not do network security or database security or OS security but
  - The ERP is treated as a “black Box” and audits focus in ERP land

Security Audits of ERP

- Focused on technical settings in the ERP such as limits
- Focused on the business functionality
- Focused on the security settings in the ERP
- Focused on ERP users / responsibilities
- Focused on separation of duties and potential conflicts of interest

Regulations and Reasons to Secure Better

- Reasons to take data security seriously
  - GDPR – Since May 2018
    - Protects citizens rights over personal data
  - Sarbanes Oxley – US parents?
    - Stops financial balance sheet reporting fraud
  - PCI – process or store cards
  - Many more…

ERPs Often Implement Security in Oracle

- ERPs have many levels of security including
  - Parameters
  - Profiles
  - ERP users and passwords
  - ERP responsibilities, roles..
  - ERP screens, menus, forms
  - SOD and COI issues are based on complex build up of permissions on multi-elements and screens
- ERPs in general control access to data through all of these components
  - This is usually not at the data level

BUT…

- Most of ERPs are implemented in the database itself as:
  - Tables,
  - Views,
  - Metadata
  - Code such as PL/SQL
- These are not controlled by ERP security controls inside of the ERP itself
  - Recursive security is missing

BUT … (2)

- The database is software running on a server or multiple servers (Unix often but can be Windows)
- The data and metadata are stored in datafiles on disk (SAN, ASM, Network Storage, Local disks)
- Users are expected to access the ERP front end but often some users are allowed:
  - Reporting interfaces
  - Development tools such as TOAD, SQL*Developer etc

Threats to an ERP Outside of the ERP

- System admins can access anything
  - Root ➔ oracle ➔ database as sysdba ➔ all data (steal PII, finance) ➔ security controls
  - Oracle ➔ database as sysdba ➔ all data (steal PII, finance) ➔ security controls
  - DBA – database as DBA ➔ all data (steal PII, finance) ➔ security controls
  - Business User database as user ➔ all data (steal PII, finance) ➔ security controls

Actual Threats

- The security of the ERP can be changed by editing metadata in ERP tables
- ERP users can have passwords reset by database UPDATE
- ERP responsibilities can be changed by INSERT, UPDATE
- ERP rule trees can be edited to allow a COI
- ERP processes (check printing?) can be run outside of the ERP

Data Theft

- Data theft can occur completely outside of ERP controls
- A DBA, admin, reporting user allowed direct access can access data outside of ERP controls
- Data can be stolen from
  - Database, SGA, redo logs, archive logs, report files, data files, test systems, network sniffing, many many more

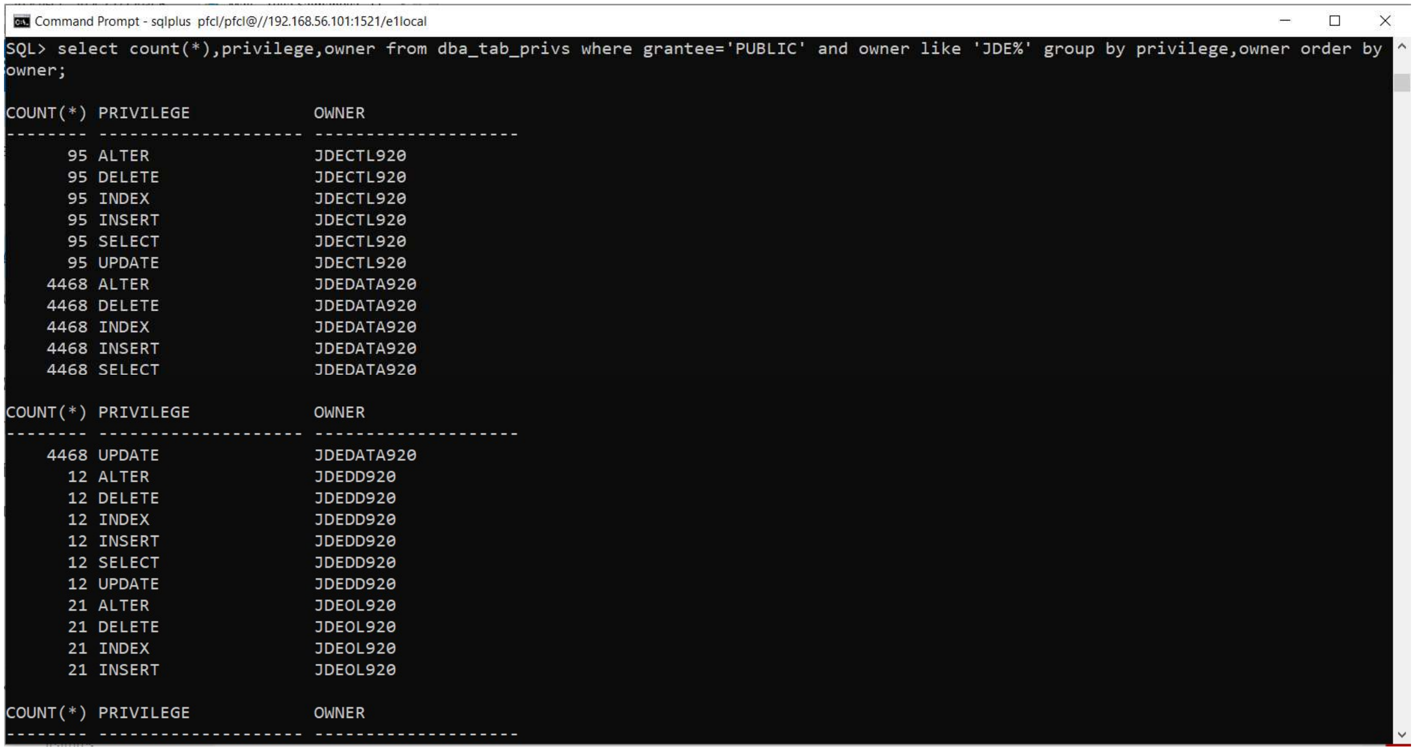
Section

Some Examples

PFCL
PETEFINNIGAN.COM LIMITED

Example: JDE Data Level Security Controls

- Literally everything except passwords are granted I,U,D,S to PUBLIC (99.9%)

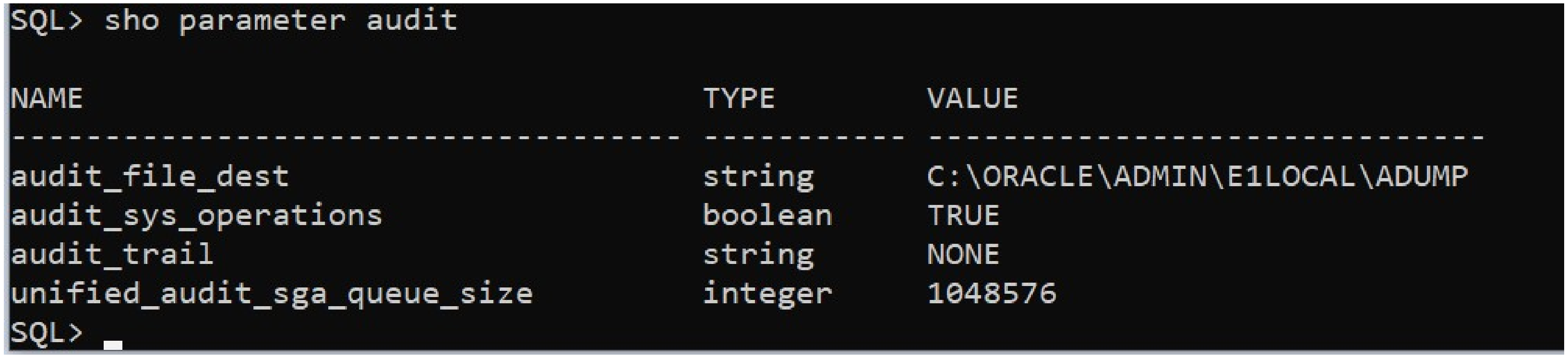


Command Prompt - sqlplus pfcl/pfcl@//192.168.56.101:1521/e1local

```
SQL> select count(*),privilege,owner from dba_tab_privs where grantee='PUBLIC' and owner like 'JDE%' group by privilege,owner order by
owner;

COUNT(*) PRIVILEGE            OWNER
-------- -------------------- --------------------
      95 ALTER                JDECTL920
      95 DELETE               JDECTL920
      95 INDEX                JDECTL920
      95 INSERT               JDECTL920
      95 SELECT               JDECTL920
      95 UPDATE               JDECTL920
    4468 ALTER                JDEDATA920
    4468 DELETE               JDEDATA920
    4468 INDEX                JDEDATA920
    4468 INSERT               JDEDATA920
    4468 SELECT               JDEDATA920

COUNT(*) PRIVILEGE            OWNER
-------- -------------------- --------------------
    4468 UPDATE               JDEDATA920
      12 ALTER                JDEDD920
      12 DELETE               JDEDD920
      12 INDEX                JDEDD920
      12 INSERT               JDEDD920
      12 SELECT               JDEDD920
      12 UPDATE               JDEDD920
      21 ALTER                JDEOL920
      21 DELETE               JDEOL920
      21 INDEX                JDEOL920
      21 INSERT               JDEOL920

COUNT(*) PRIVILEGE            OWNER
-------- -------------------- --------------------
```

Example: JDE Database Level Audit Trail

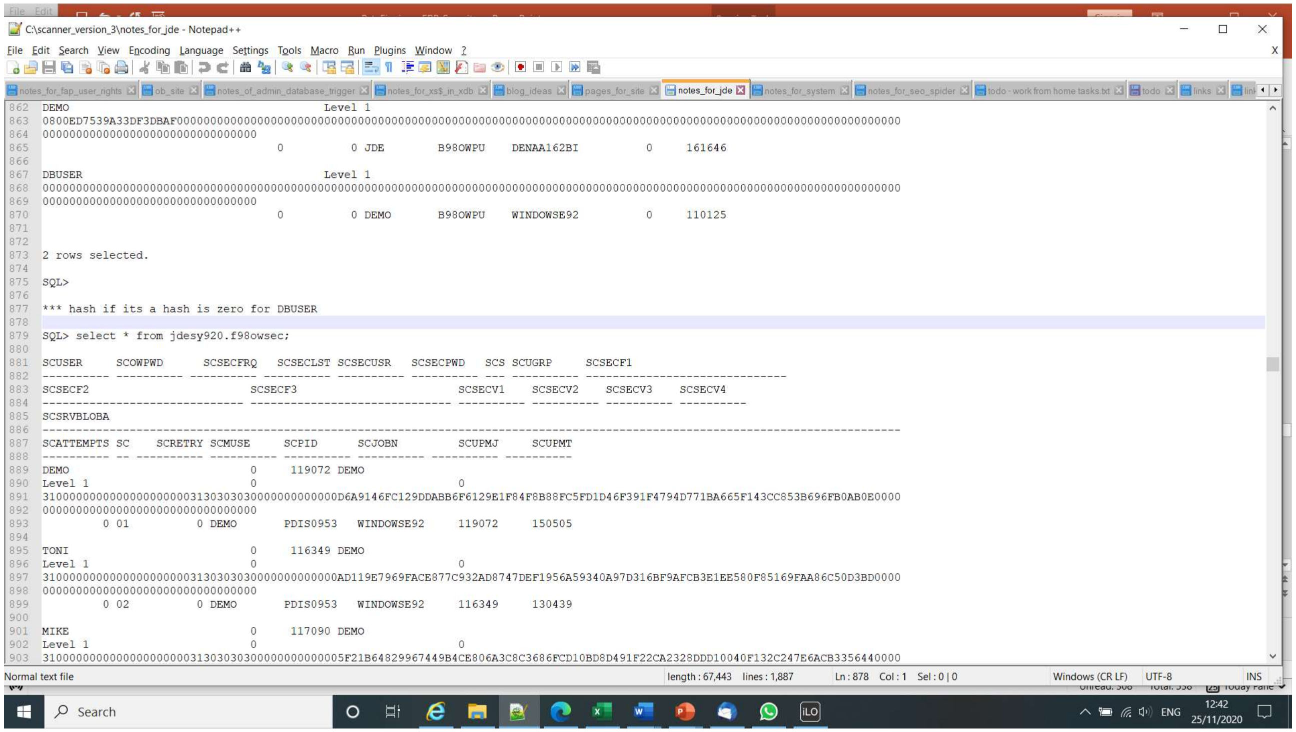
- A sample JDE installation has no database level audit trails
- SYSDBA audit is enabled but this does not track data level actions by other users



```
SQL> sho parameter audit

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      C:\ORACLE\ADMIN\E1LOCAL\ADUMP
audit_sys_operations                 boolean     TRUE
audit_trail                          string      NONE
unified_audit_sga_queue_size         integer     1048576
SQL> _
```

Example: JDE Critical Security Could be Changed

- A very small percentage of critical tables are not granted to PUBLIC in JDE but DBA can change!


C:\scanner_version_3\notes_for_jde - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
notes_for_fap_user_rights
ob_site
notes_of_admin_database_trigger
notes_for_xs$_in_xdb
blog_ideas
pages_for_site
notes_for_jde
notes_for_system
notes_for_seo_spider
todo - work from home tasks.txt
todo
links
Normal text file
length : 67,443 lines : 1,887
Ln : 878 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS
Search
ENG
12:42
25/11/2020

```
DEMO                                      Level 1
0800ED7539A33DF3DBAF000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000
                                   0          0 JDE        B98OWPU    DENAA162BI          0     161646

DBUSER                                    Level 1
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000
                                   0          0 DEMO       B98OWPU    WINDOWSE92          0     110125


2 rows selected.

SQL>

*** hash if its a hash is zero for DBUSER

SQL> select * from jdesy920.f98owsec;

SCUSER     SCOWPWD      SCSECFRQ   SCSECLST SCSECUSR   SCSECPWD   SCS SCUGRP     SCSECF1
---------- ---------- ---------- ---------- ---------- ---------- --- ---------- ------------------------------
SCSECF2                        SCSECF3                        SCSECV1    SCSECV2    SCSECV3    SCSECV4
------------------------------ ------------------------------ ---------- ---------- ---------- ----------
SCSRVBLOBA
--------------------------------------------------------------------------------------------------------------------------------
SCATTEMPTS SC    SCRETRY SCMUSE     SCPID      SCJOBN         SCUPMJ     SCUPMT
---------- -- ---------- ---------- ---------- ---------- ---------- ----------
DEMO                           0     119072 DEMO
Level 1                        0                              0
31000000000000000000003130303030000000000000D6A9146FC129DDABB6F6129E1F84F8B88FC5FD1D46F391F4794D771BA665F143CC853B696FB0AB0E0000
00000000000000000000000000000000
         0 01          0 DEMO       PDIS0953   WINDOWSE92     119072     150505

TONI                           0     116349 DEMO
Level 1                        0                              0
31000000000000000000003130303030000000000000AD119E7969FACE877C932AD8747DEF1956A59340A97D316BF9AFCB3E1EE580F85169FAA86C50D3BD0000
00000000000000000000000000000000
         0 02          0 DEMO       PDIS0953   WINDOWSE92     116349     130439

MIKE                           0     117090 DEMO
Level 1                        0                              0
310000000000000000000031303030300000000000005F21B64829967449B4CE806A3C8C3686FCD10BD8D491F22CA2328DDD10040F132C247E6ACB3356440000
```

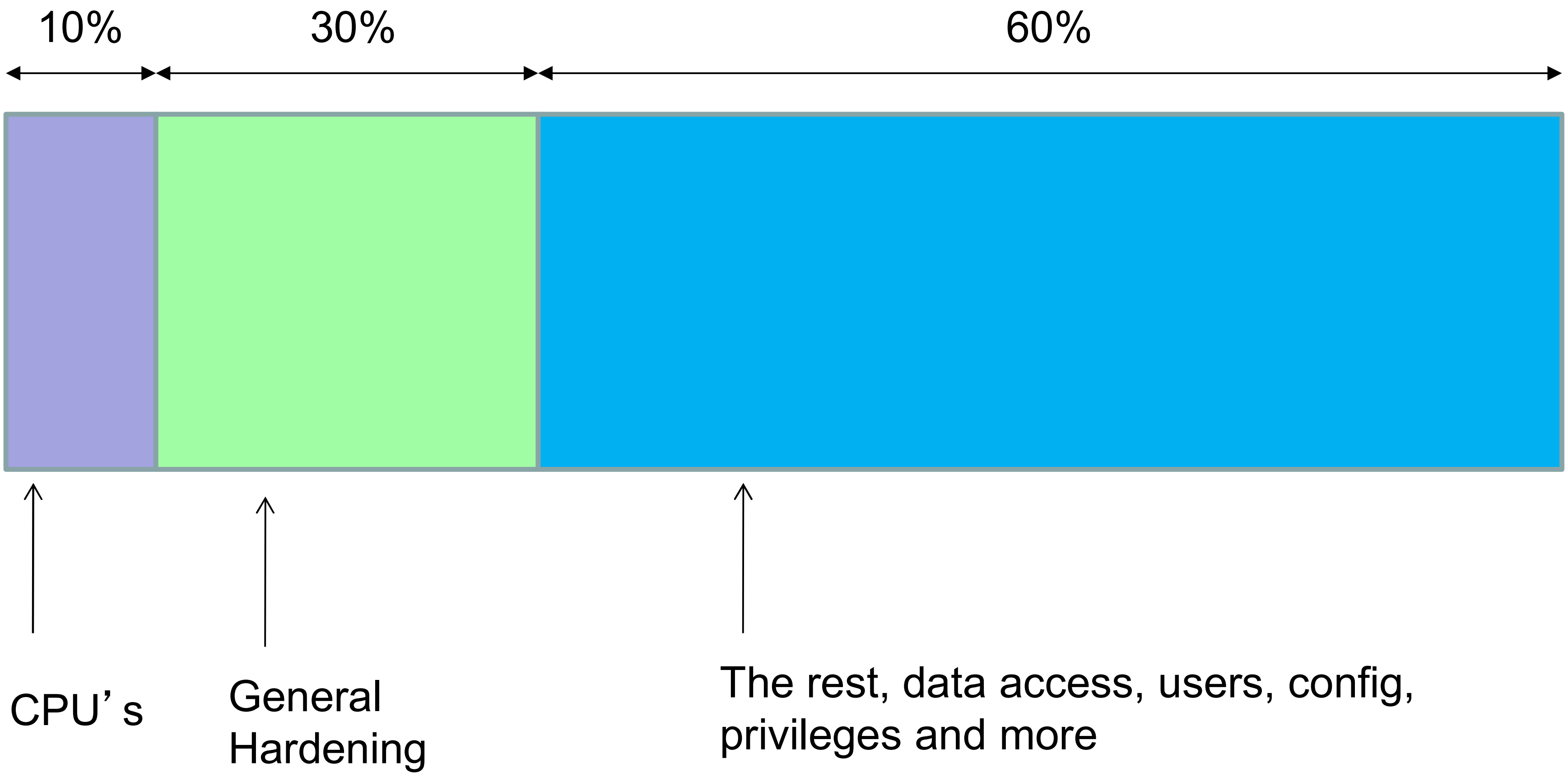
Section

Secure Data in an ERP

We Must Secure the Database and Server

- To properly secure an ERP **we must also**:
  - Secure the operating system
  - Secure the core database against general threats
  - Secure the core database against ERP level threats
  - Secure the network between the ERP and the database (often not segregated or encrypted)

Database Security High Level



10%

30%

60%

CPU's

General Hardening

The rest, data access, users, config, privileges and more

Threats – Platform and Data

- There are two key threats
- **Data Theft:** The attackers goal is to steal your data, PII, Cards, Health, Business confidential or more
- **Platform Access:** The attacker is not interested in your data or simply does not see the value in it. Instead he sees your Oracle database as an easy target to attack and from there to access what he really wants – other services, websites or more
- **Therefore we must protect data as a key task but we must not neglect the Oracle platform as a potential target and lock it down as well**

Securing A Database is Complex

- The focus for years is on hardening and patching – CPU and CIS for instance
  - This is fine BUT it does not secure your data at all
- Data security is harder to do as its specific
- User level security – permissions, profiles
- Access controls – grants, roles, objects
- Context based security
- **We must consider ERP data in the database**

Implement Comprehensive Audit Trails

- In general ERP systems usually have some level of audit trails at the ERP level
- The database engine does not audit itself generally
- We must implement audit trails in the database using standard audit, Unified audit, FGA or triggers
- We must also audit the data itself in the database
- We must audit ERP security (metadata and controls)
- You must be able to find out if someone abuses the ERP from the database

Layers of Database Security

- Patch
- Harden
- User rights / control = Least Rights
- Data access controls = Least Right
- Access controls to the database
- Context based security
- Secure Coding

Context Based Security

- ERP controls do not control access to data tables
- Database table level controls are too granular
- Context based controls needed
- Can use Oracle products – DV, VPD, OLS, TSDP, …
- Can also use encryption as a context control
- Home grown controls can be created using triggers, views, procedures and contexts

Conclusions

- ERP security is generally in the ERP
- The assumption is that the ERP is controlled at the ERP level
- We must understand that an attacker (or employee) can access data or security directly in the database or operating system
- We must secure the core database
- We must secure the ERP in the database
- We must implement audit trails in the database

Questions

If Anyone has questions, please ask now or catch us after the event!!

Data Security in ERP

and Other Large Business Systems