

Appreciation of Auditing and Securing Oracle

Security Design



Legal Notice

Appreciation and Auditing and Securing Oracle

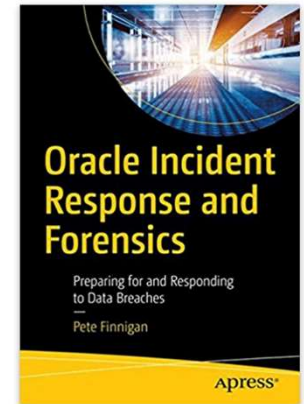
Published by
PeteFinnigan.com Limited
Tower Court
3 Oakdale Road
York
England, YO30 4XL

Copyright © 2018 by PeteFinnigan.com Limited

No part of this publication may be stored in a retrieval system, reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, scanning, recording, or otherwise except as permitted by local statutory law, without the prior written permission of the publisher. In particular this material may not be used to provide training of any type or method. This material may not be translated into any other language or used in any translated form to provide training. Requests for permission should be addressed to the above registered address of PeteFinnigan.com Limited in writing.

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.



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

- Where does Oracle fit in cyber security?
- Attacks against Oracle
- How should we secure Oracle?
- GDPR, Multitenant and cloud
- Conclusions



Bragging Rights, Government Sponsored?

- Back in the 1980's people like Phiber Optik - https://en.wikipedia.org/wiki/Mark_Abene and Erik Bloodaxe [https://en.wikipedia.org/wiki/Erik_Bloodaxe_\(hacker\)](https://en.wikipedia.org/wiki/Erik_Bloodaxe_(hacker)) (Chris Goggans)
 - Were in the hacking game for the buzz but ended up breaking the law and going to prison (Mark)
- Some people are still 1980s hackers – Lauri Love, Gary McKinnon
- Government Hacking
 - Edward Snowden – copied and leaked CIA, NSA highest level data in 2013 - https://en.wikipedia.org/wiki/Edward_Snowden and ran to Hong Kong and then Russia
- 400gb of emails, documents, embarrassing information and most importantly the hacking toolkit **Remote Control System (RCS)** they sell to countries stolen – Phineas Fisher



<https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-june-2018-145942680-records-leaked/>

Data Hacks are Now Commonplace

- The number of data breaches rises daily
- Breaches are so common now that they are **normal news** and not **niche news** anymore
- Even the BBC no longer brings on a security expert to talk about the latest breach
- Data breaches in:
 - April 2018 – 76,611, 721 records breached
 - May 2018 – 17,273,571 records breached
 - June 2018 – 145, 942, 680 records breached
- I personally have been involved in post breach investigations involving Oracle database systems

I had a conversation with a taxi driver w/c 20/8/2018 and he didn't know what a data breach was BUT proceeded to tell me how he was scammed out of a loan payment. That is the result of a beach ultimately

The Rise of Data Regulations

- Regulatory bodies now taking data breaches much more seriously
 - In the USA most states have copied the California 1386 data breach laws
 - Sarbanes Oxley (SOX), Health Insurance Portability Act (HIPPA) and Gramm Leach Bliley (GLBA), PCI,...
 - In the EU each of the 28 member states have implemented the new data protection law called GDPR
 - This will bring much stronger data protection laws and 20M Euro or 4% GDP fines
 - Far reaching; requires active consent, breach notification, knowledge of a breach, users rights...

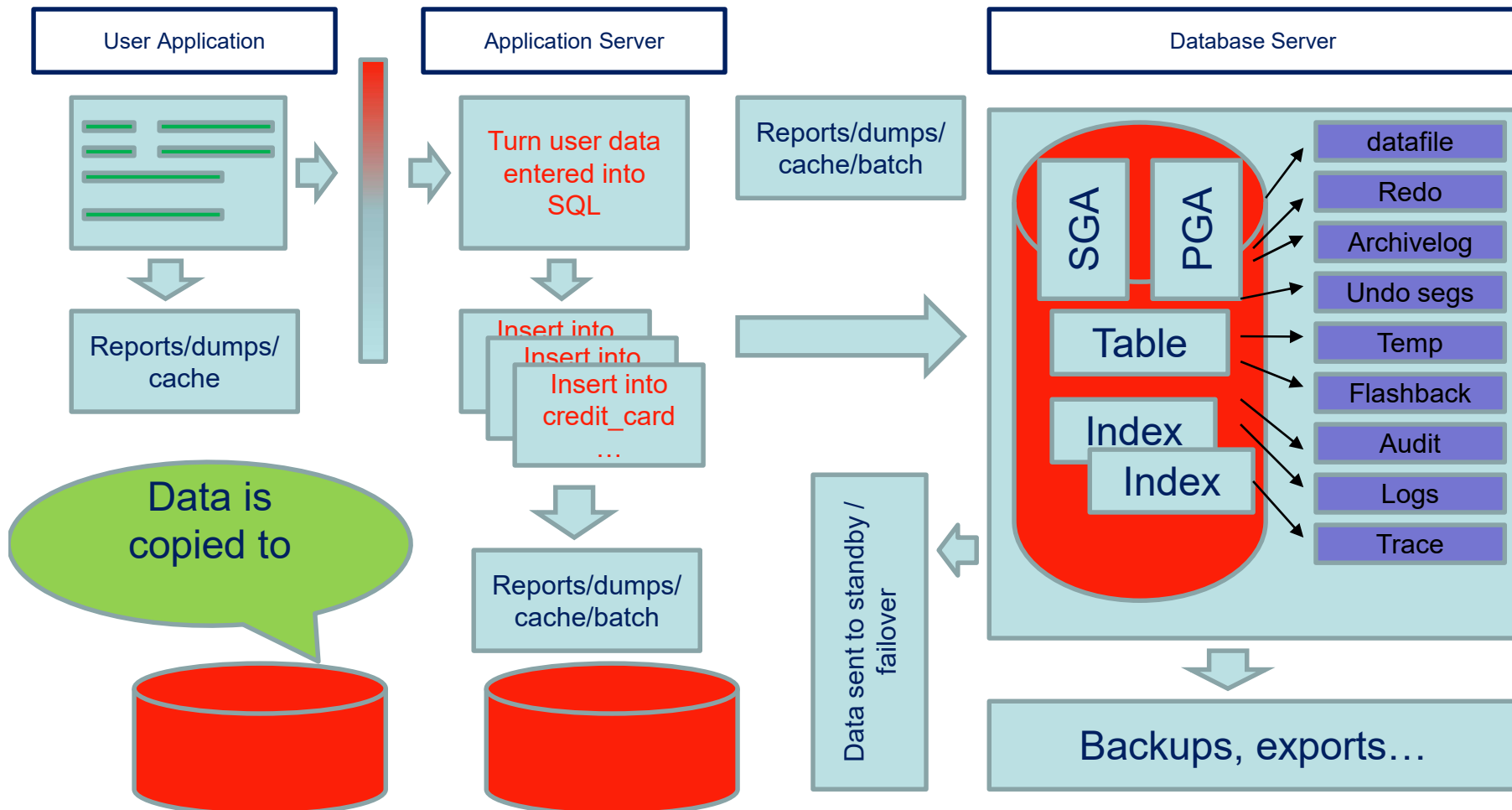
Oracle and Security

- Oracle has always been associated with security
 - This is not what it first seems – their first customers were three letter agencies
- Oracle went after software security certifications
 - Meaningless for customers – they don't secure your data
- Oracle refused to have regular security patches until 2005
- The first patches were alerts 13 to 68 from 2001 to 2005 (I was credited in some of them #68 for instance)
- There are still alerts now – **out of step security patches**
- I wrote the first major Oracle security paper in 2001
- I wrote the first papers on SQL Injection in Oracle 2002
- Securing databases has not matured enough in 18 years

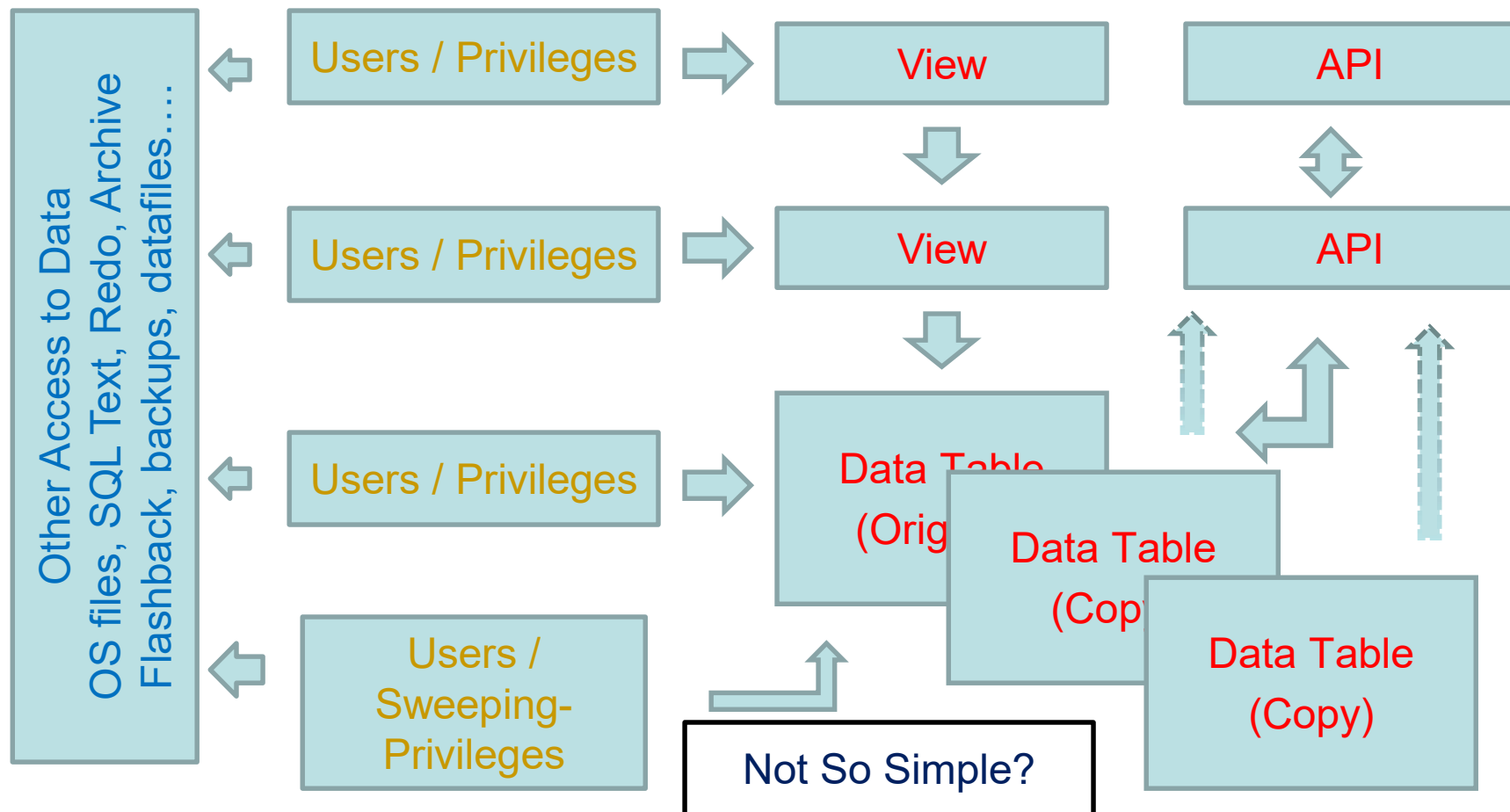
The Current State From Oracle

- Oracle is a very generic engine whose purpose is to process your data and host your applications
- **The big surprise to some people is that Oracle do not secure your data for you**
- Usually I see in customer databases
 - No Patching, No data security, No hardening
 - No user least rights, No audit trail
- A default database is not secure (44k default PUBLIC grants)
- **Oracle security products such as Database Vault are not free (except in 18c XE, amazing!!)**
- BUT, these security products are just applications and must also be secured – no one realises this

Understand Oracle - Where Is The Data?



Copies of Data and Multiple Access Paths




Attack Types are Many

- The possibilities are vast and complex:
 - The rise of SQL / PL/SQL / DDL ... Injection
 - Password / authentication abuse
 - IPR loss
 - Data loss due to leakage (out of the database) or permissions
 - Abuse defaults
 - Abuse permissions
 - **Some attacks are not hackers**
 - DBAs use SYSDBA 95% of sites I see
 - No audit trails – no accountability – only 10 – 30% of sites

Steal the cards by
decrypting via SQL Injection

Hack The Credit Card Details



The screenshot shows a blog post titled "Oracle Security Services" with two entries. The first entry is titled "CardNumber-Mr David Bentley-4049877198543457" and the second is "CardNumber-Mr Martin Chisholm-3742345698766678". A yellow box highlights the SQL injection payload used to extract the card numbers. A blue arrow points from the payload box to the search input field on the right side of the page, which contains the same payload.

Oracle Security Services

October 27, 2013

X
Filed under: Uncategorized — pete @ 12:00 am [Edit This](#)

CardNumber-Mr David Bentley-4049877198543457

[Comments \(0\)](#)

X
Filed under: Uncategorized — pete @ 12:00 am [Edit This](#)

CardNumber-Mr Martin Chisholm-3742345698766678

[Comments \(0\)](#)

Hack string:

```
x%'))))a)/**/union/**/select/**/33,1,to_timestamp('27-OCT-13'),to_timestamp('27-OCT-13'),'CardNumber-||name_on_card||'-||bof_kkrc.dr(cc34),'x',0,null,'publish','open','open',null,'name',null,null,to_timestamp('27-OCT-13'),to_timestamp('27-OCT-13'),null,0,null,0,null,null,0,6/**/from/**/orablog.b of_pay_details--
```

pages
about
contact page

blogroll
oracle security expertise
pfciscan

categories:
uncategorized
uncategorized
oracle security
general

search:
x%'))))a)/**/union/**/sele

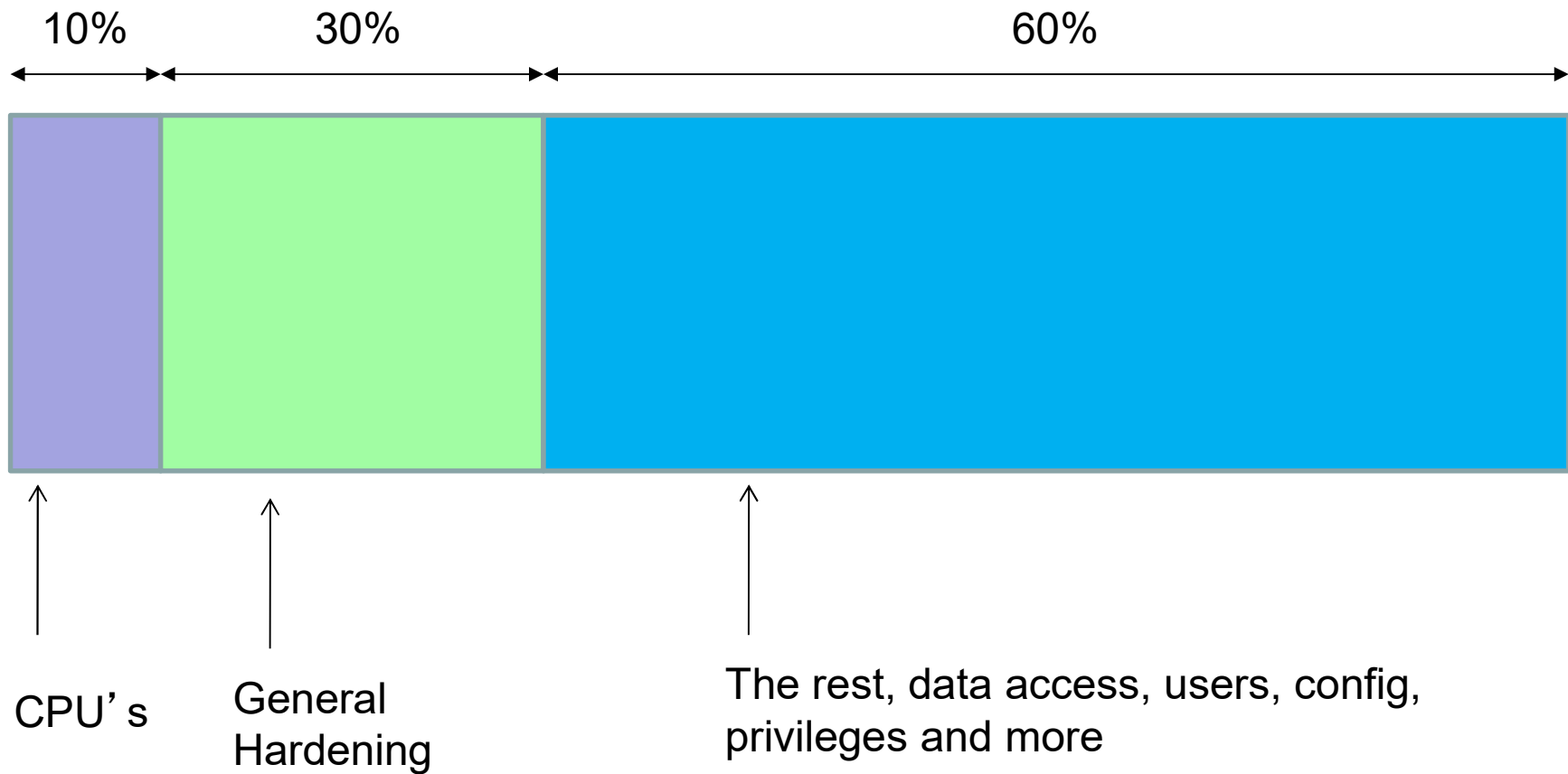
archives:
march 2008
may 2008
october 2013
december 2013

meta:
site admin
layout
rss
comments rss
valid xhtml
xfn
ob

Countermeasures

- A counter measure is the actions that you take to prevent a threat becoming real – i.e. reducing the risk of the threat
- A countermeasure in the Oracle database can be:
 - Hardening
 - Permissions
 - Audit trails
 - Application of patches
 - Security design
- Something that makes the database more secure by blocking or preventing threats from becoming risks

Compartmentalise Data Security?



What Is Oracle Security?

- It is not Oracle's Security
- It is **our** security of **our** data

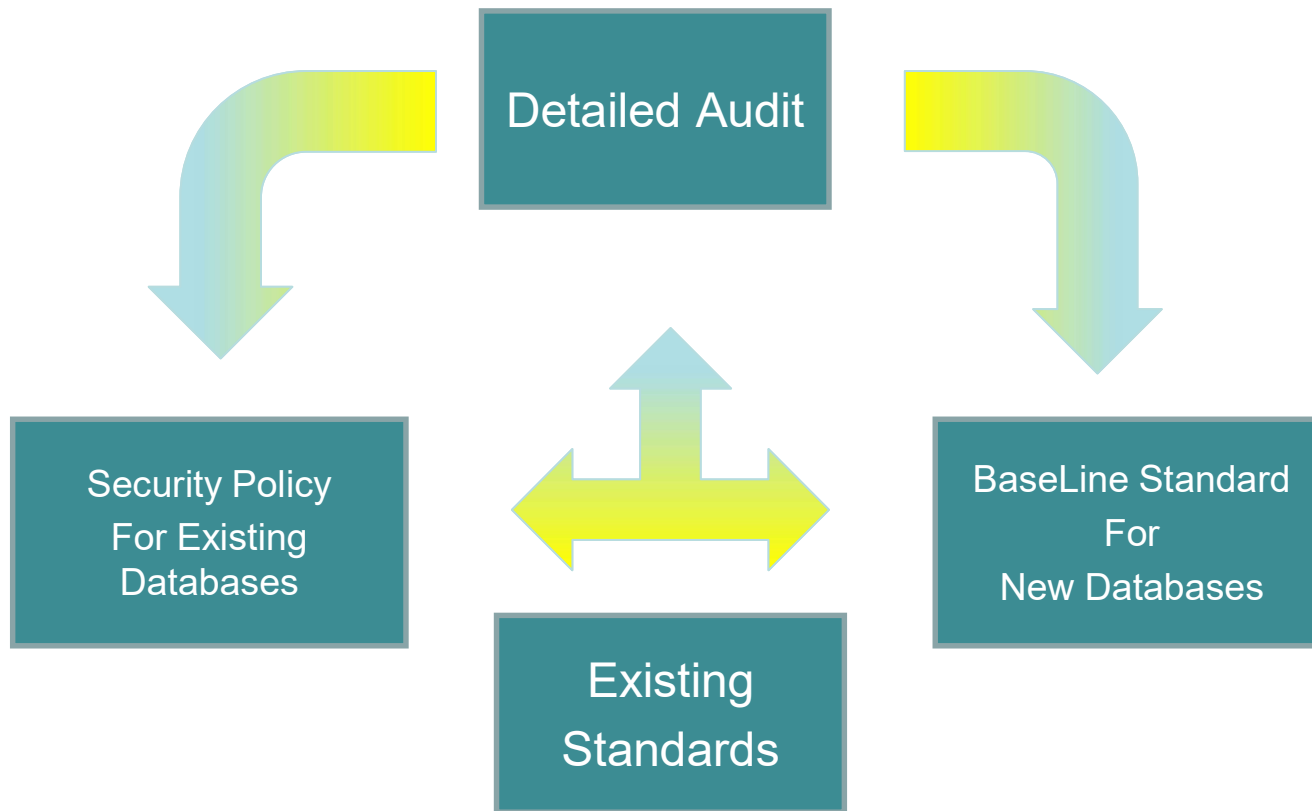
Threats - Platform And Data Security

- 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**

What is Data Security?

- Data security is the understanding of and protection of the actual data in your database
- This means you must know what that data is and who accesses it and how and when and why
- You do not need to secure all data - just important data
- You must understand all access paths to the data
- You must understand if multiple copies exist and where (not just in the database)
- Data security is not just about `GRANT SELECT ON SCOTT.CREDIT_CARDS TO FRED`

What Is Involved In Securing A Database?



Perspective

- What do we wish to achieve?
- We must understand what we are trying to protect and why
- We must consider money – budget, practicality, complexity of choices and solutions
- We must understand hackers, Oracle, our existing designs and more
- We must plan to secure all data – no point in securing one copy if another is freely available to an attacker
- We must consider formality – policy, compliance, testing, monitoring
- Oracle Security is big and complex

Tasks

- Identify budget
- Identify and understand risks
- Make a formal Plan / Policy for securing all data
- Identify solutions for each clause
- Understand individual options, tools, cost options, third party options available
- Implement
- Test for compliance
- Repeat

Actors

- To assess security of data in an Oracle database we must know who the “actors” are – not Johnny Depp but
 - Direct access persons –
 - job roles that are allowed to connect to the database and why
 - Individuals who are allowed to connect and why – when its not a clear job role
 - Processes –
 - Feeds and extracts
 - Business tasks –
 - Reporting
- Unless we know about who connects and why we cannot secure the Oracle database

Does Patching and Hardening Work?

- If I applied all clauses of the CIS benchmark would my credit card data still be hackable?
- If I applied the latest Oracle Security patches (CPU / PSU) would my credit card data be hackable?
- **The answer is YES**
- This means that hardening and patching in a database are not as important as good data security design
- Hardening targets simple default grants but in Oracle there are many ways to bypass this
- Patching and hardening does not stop users with credentials from exploiting bad design

Hardening Examples

```
[Enter value for object_to_test: UTL_FILE
```

```
[Enter value for owner_to_test: SYS
```

NAME	OWNER	TYPE
UTL_FILE	SYS	PACKAGE BODY
DBMS_SCHEDULER	SYS	PACKAGE BODY
KUPW\$WORKER	SYS	PACKAGE BODY
KUPM\$MCP	SYS	PACKAGE BODY
KUPF\$FILE	SYS	PACKAGE BODY
DBMS_CUBE	SYS	PACKAGE BODY
DBMS_AW_EXP	SYS	PACKAGE BODY

```
7 rows selected.
```

- Just one example; revoke execute on UTL_FILE; this package is accessible via other means

Revoke on ALL_USERS

```
SQL> select distinct owner from all_objects;
```

```
OWNER  
-----  
OWBSYS_AUDIT  
TKT_TEST  
SQL92  
MDSYS  
DEV  
ORABLOG  
ILO  
FACADM  
PUBLIC  
OUTLN  
CTXSYS  
OLAPSYS  
FLOWS_FILES  
OWBSYS  
HR  
TKT_DEV  
DEV2  
CCKEY  
SYSTEM  
ORACLE_OCM  
EXFSYS  
APEX_030200
```

- Old clause not in current standard but a good example
- Maybe we do not see all users but we can find most
- There are too many ways to get the same information in Oracle
- In the case of files we could use Java; C and more
- **In the case of files we need to protect the key not the door lock**

Hardening CIS as an Example

- Default passwords but not remove default users except samples
- No Password check for other users
- Patches suggests to use opatch – **hmmmm**
- Parameters 19 are checked in 12c, I check more than 60!
- 12c in CIS does not include all the new PDB parameters
- 12c for revoke EXECUTE and SELECT does not include any 12c views
- USER\$ is included but no EXU%USR views
- DBA is included but not IMP_FULL_DATABASE
- ALTER USER is not included
- No CDB% views
- No %_AE views
- ALTER SESSION not included

Focus on

- Stop people connecting to Oracle
 - Network controls – sqlnet.ora, listener, init parameters
 - Logon triggers
- User rights
 - Remove all default users not needed
 - Remove all users that are not needed
 - Aim for least privileges of accounts that remain
- Data access controls
 - One copy of data
 - Enforce table level grants
 - Enhance with context based security
- Enable identity and audit trails
- Use context based security and don't abandon hardening and patching completely

It is possible to simulate most of this for free with core features such as views and triggers

Additional Security Cost Options from Oracle

- Database Vault – primary tool to protect against privilege accounts and to put realms around data/function
- Oracle Label Security - Allows data to be accessed by row level labels and the users current label access level
- Data Redaction (ASO) – Redact some data from end users – black like through data!
- Transparent Sensitive Data Protection – create classes of sensitive data to allow more centralised way of protecting sensitive data – uses VPD and Data Redaction
- Transparent Database Encryption – allows data to be encrypted at rest – either at tablespace level or at the column level
- Oracle Data Masking – find data to mangle / obfuscate and specify rules to then change that data – keeping referential integrity
- Audit Vault and Database Firewall– centralised database for audit storage including certificate based confirmation of data

The Future

- GDPR focuses on data security
 - Data security by design
 - Data security by default
 - Audit trails
 - Incident response
- Multitenant
 - Forces us to manage two databases instead of one
 - Focus on core database as though its legacy and then consider the COMMON users, roles, grants, etc
- Cloud
 - Audit as though a legacy on premise database
 - Then consider cloud
 - Producer, consumer, location, encryption, network

Conclusions – 5 takeaways!

- Data security design **MUST** come first
- Hardening does not do what you think it does in Oracle – too many ways to get around it and has much lower value than say an OS
- Understand how Oracle works – data leaks!
- Understand the many threats not just SQL Injection
- Create a data security policy first then build, check and test against it. Plan not made up

Appreciation of Auditing and Securing Oracle

Security Design