UKOUG UNIX SIG

September 8th 2010

Oracle Security

The Right Approach (IMHO) – Part 1

By

Pete Finnigan

Updated Wednesday, 1st September 2010

Why Am I Qualified To Speak

- PeteFinnigan.com Ltd, Est 2003.
- http://www.petefinnigan.com
- First “Oracle security” blog.
- Specialists in researching and securing Oracle databases providing consultancy and training Database scanner software authors and vendors.
- Author of Oracle security step-by-step book; co-author of Expert Oracle practices, author of HSM/TDE Book to be published soon.
- Published many papers, regular speaker (UK, USA, Slovenia, Norway, Iceland, Finland and more).
- Member of the Oak Table Network.

Agenda

- Two Parts to this presentation
- Background “glue”
- The correct approach (IMHO) – The message
- Exploit + reaction (a number of levels)
  - downloadable, easy
  - Realistic theft
  - Sophisticated attack
  - Data analysis
  - User Analysis
- Conclusions

Introduction

- You have me for 1.5 hours (2 sessions)
  - The focus is “***how easy it is to steal***” [some examples] and “***how easy it is to not secure properly***” [examples]
  - But I want to give you some examples
  - And; we are going to try a lot of demos!
  - So timing may be out a little, so the split between part 1 and 2 may move slightly

Overview

- What do I want to achieve this evening
  - I want you to "grasp" some of the basic ideas behind securing an Oracle database – I will say what they are at the end BUT see if you can pick them up
- Anyone can secure an Oracle database BUT we should get the ground rules right and really understand why to secure and how to secure
- **Ask questions any time you would like to**
- Try out some of the tools and techniques yourself later on or now if you have a local Oracle database on a laptop (NOT ALL OF THEM ON PRODUCTION!)

What Is Oracle Security?

- Securely configuring an existing Oracle database?
- Designing a secure Oracle database system before implementation for new databases?
- Understanding what you have – perform an audit?
- Using some of the key security features
  - Audit facilities, encryption functions, RBAC, FGA, VPD…
- Oracle security is about all of these BUT
  - **It is about securely storing critical / valuable data in an Oracle database. In other words its about securing DATA not securing the software!**

Traditional Security Approach

- Hardening by checklist – good idea?
- A number of them available
  - SANS Step-by-step guide
  - SANS S.C.O.R.E.
  - CIS benchmark
  - DoD Stig
  - IT Governance book
  - Oracle's own checklist

Problems With Checklists

- Not many checklists exist for Oracle databases
- Most are from same initial source or are very similar
- Some structure there but not good enough
  - “tip based rather than method based”
- Lists don’t focus on securing the data
- Difficult to implement for a large number of databases
- CIS for instance has 158 pages

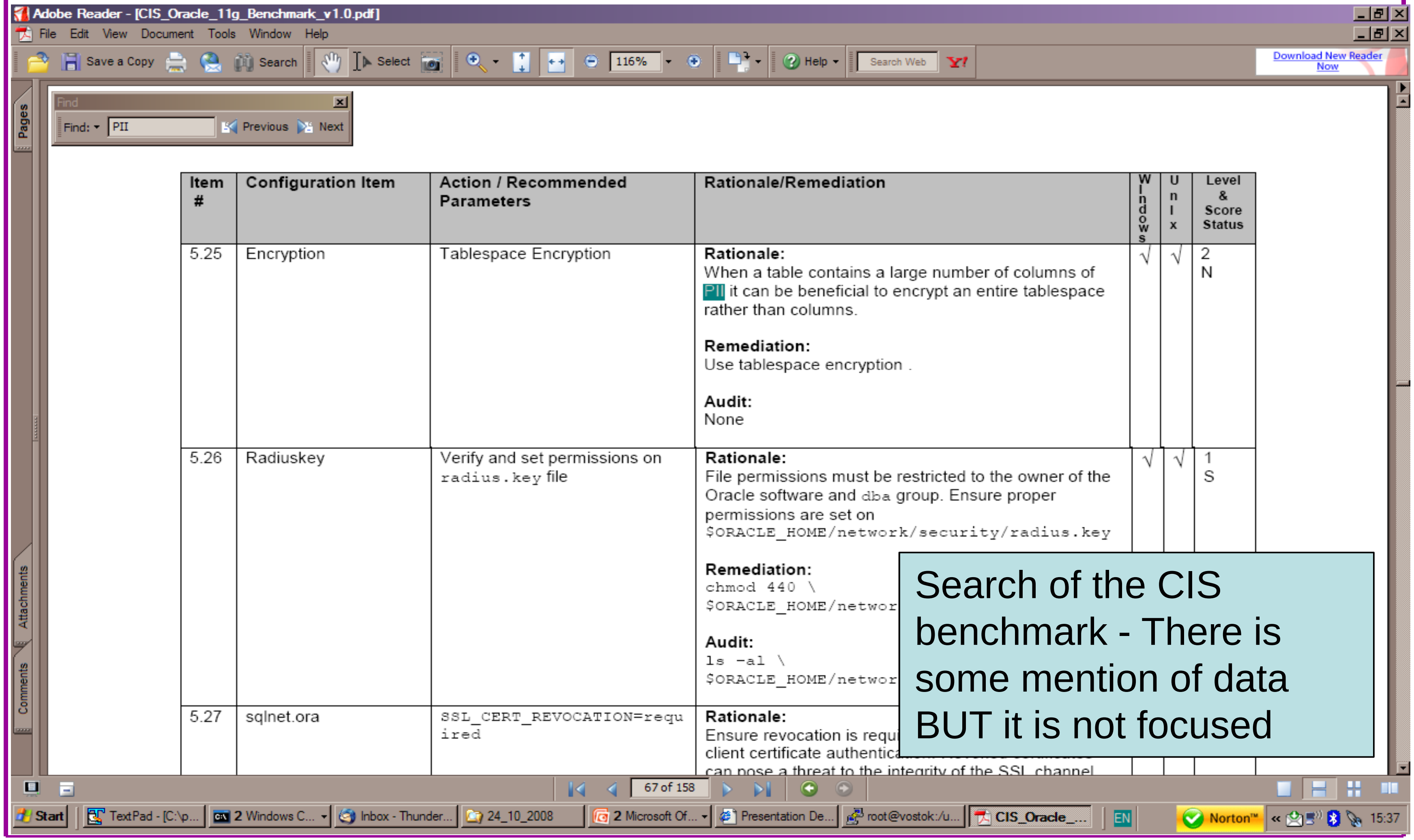
Solutions are not Simple

- Time based solution
  - Could spend man years on even a single database
  - Finding solutions for each issue is not as simple as applying what it says in the document
- Clever solutions are needed
  - Technical solutions need to be specified
  - Onion based approach is good
  - Basic hardening in parallel

Examples Of Problems

- Two examples:
  1) Check 3.0.2 in CIS states “all files in $ORACLE_HOME/bin directory must have privileges of 0755 or less – fine - but the solution states “chmod 0755 $ORACLE_HOME/bin/*” – is it a good idea?
  2) Solutions are not as simple as indicated. For instance fixing a weak password should also include, fix the password, management, hard coded passwords, audit, policy….

Checklists And PII Data



Find: PII

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
5.25	Encryption	Tablespace Encryption	**Rationale:** When a table contains a large number of columns of PII it can be beneficial to encrypt an entire tablespace rather than columns. **Remediation:** Use tablespace encryption . **Audit:** None	√	√	2 N

5.26	Radiuskey	Verify and set permissions on `radius.key` file	**Rationale:**
			File permissions must be restricted to the owner of the Oracle software and `dba` group. Ensure proper permissions are set on `$ORACLE_HOME/network/security/radius.key`
			Remediation:
			`chmod 440 \`
			`$ORACLE_HOME/networ`
			Audit:
			`ls -al \`
			`$ORACLE_HOME/networ`
				√	√	1
						S

5.27	sqlnet.ora	`SSL_CERT_REVOCATION=required`	**Rationale:** Ensure revocation is requi client certificate authentica can pose a threat to the integrity of the SSL channel			

Search of the CIS benchmark - There is some mention of data BUT it is not focused

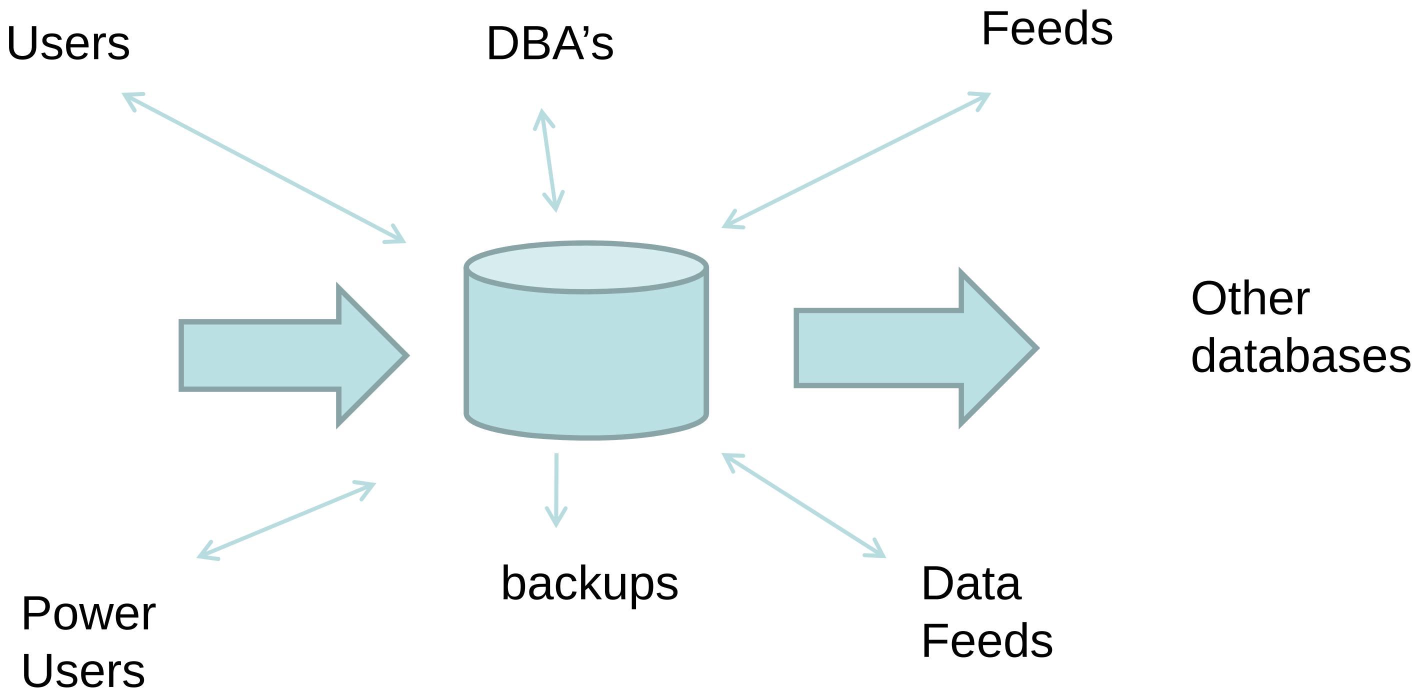
The Right Method To Secure

- Start with “**the data**”
- Understand “**data flow**” and “**access**”
- Understand the problem of securing “**your data**”
- Hardening should be part of the solution **BUT** not **THE** solution
- Checklists do not mention “**your**” data

Complex But Simple Solutions Needed

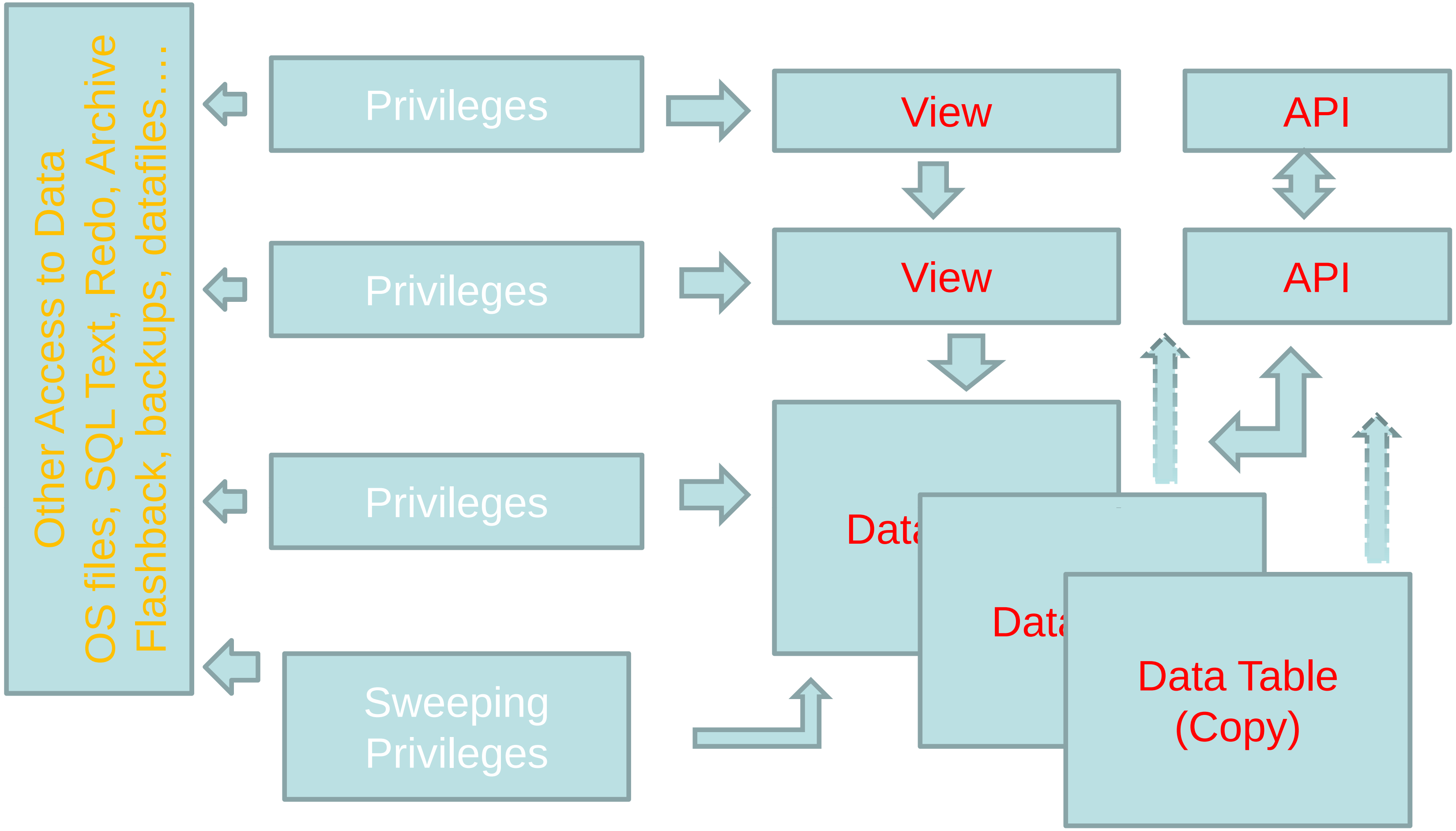
- Overarching solutions are needed
- Remove all types of access from the data
- Ensure only those who should see, can see the data
- Unfortunately it’s not that simple as there are:
  - Many paths to the data
  - Many copies of data
  - Data stored or in transit that is accessible
  - Data copied outside of the database

Understand Architecture



Identify each type of person and a sample account for each

Data Access Models



Data Access Is Not “Flat”

- Data model is not flat – remove the “blinkers”
- Access rights are also not flat
- Data is often replicated
  - In other tables – in interfaces – flexfields …
  - Indexes
  - Shared memory
  - Data files
  - Operating system
  - Many more…

How / Who

- The data must be identified (found?)
- The access paths must be found
- The “people” – real people identified
- Map to these to database user accounts
- Assess who can access data and how
- Only now can we hope to secure data

Database Security Focus

- If you are a hacker what is the focus?
  - Lots of bugs to study
  - Lots of exploits for download
  - Lots of info on hacking Oracle to use
- If you are a defender what is the focus?
  - In my experience not much has been done
  - People rely on Oracle doing the work BUT they don’t!

More for the Attacker

- Lots of databases have these issues:
  - Weak and guessable passwords
  - No password management (fixed from 11gR1 and 10.2.0.2)
  - Weak controls on the data and functions
  - No audit in the database (fixed from 11gR1 and 10.2.0.2)
  - Weak privilege design for users, solutions (batch, feeds etc) and DBA's
  - Usually no processes to manage any breach or potential breach

Simple Exploit

- Escalation of Privileges
- 5 minutes demonstration

Live Demo 1

What are the issues?

- For you:
  - – Easy to down load
  - – Easy to run
  - – No skill needed
  - – Everyone can learn about it and download
  - – Only real solution is patch (for most bugs / exploits)
  - – BUT.....

Payloads, Targets

- The focus of researchers is “grant DBA to public”
- This is wrong, the possible payloads are infinite
- The “real” target is
  - Data
  - Job satisfaction
  - Revenge
  - More?
- Factor in IDS evasion
- Factor in downloadable exploits benefit those who “already know something”...

Stealing Data - Realistic

- We are now going to demonstrate a much more realistic case of simple data theft
- This is more realistic because real systems audited by us allow this to happen – indeed we know theft using techniques like this has happened

Breach - Slide 2

- Hacking an Oracle database to “steal”
- 15 minutes demonstration

Live Demo 2

Any Questions?

Contact - Pete Finnigan

PeteFinnigan.com Limited
9 Beech Grove, Acomb
York, YO26 5LD

Phone: +44 (0) 1904 791188
Mobile: +44 (0) 7742 114223
Email: pete@petefinnigan.com