
# User Least Privilege

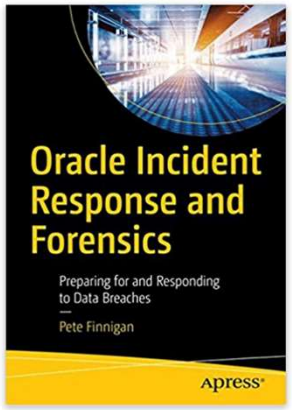
UKOUG – Liverpool 2018


# Legal Notice

## Hardening Oracle

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

PFCL
PETEFINNIGAN.COM LIMITED




# Pete Finnigan – Background, Who Am I?

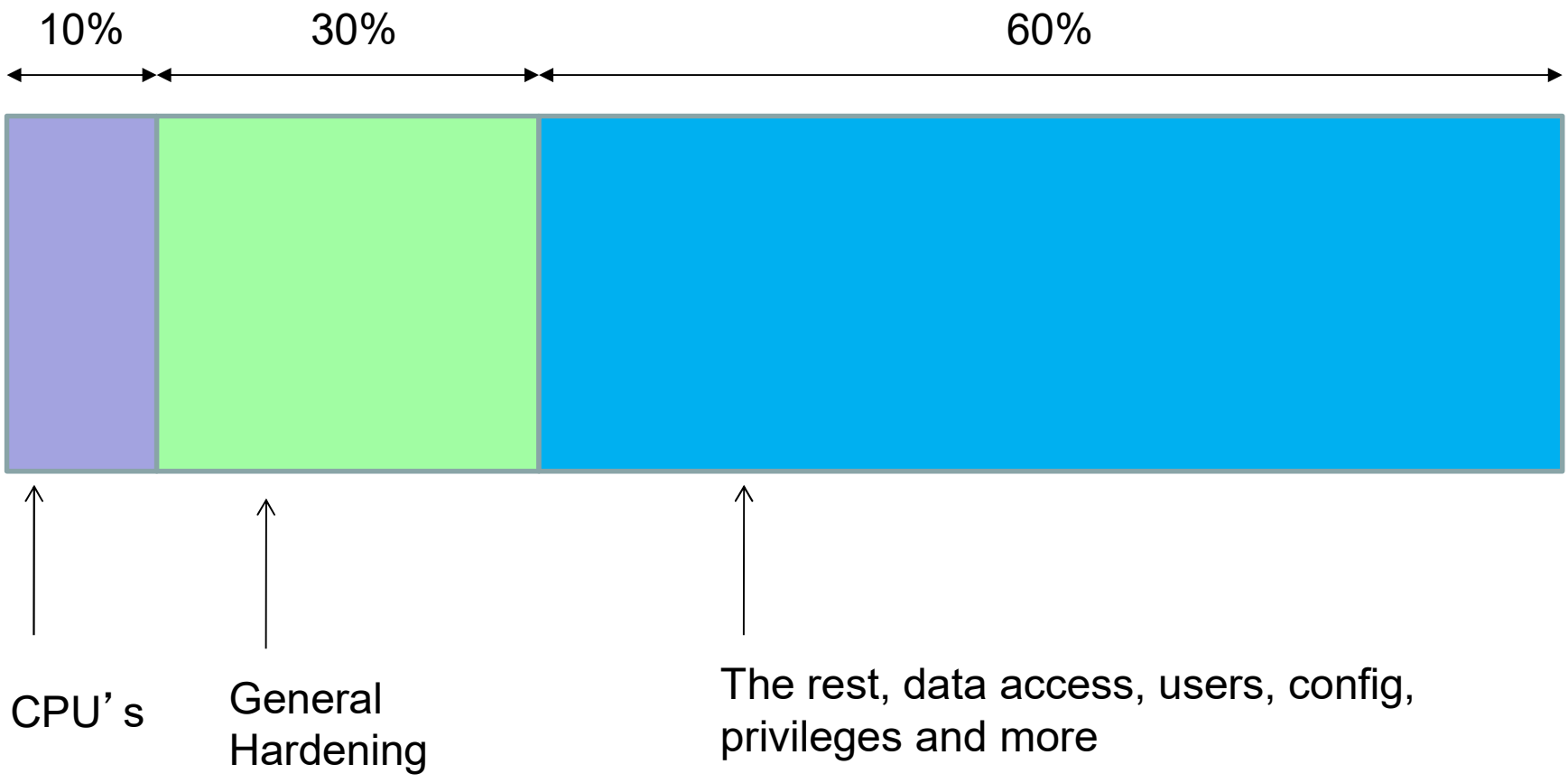
- Oracle Security specialist and researcher
- CEO and founder of PeteFinnigan.com Limited in February 2003
- Writer of the longest running Oracle security blog
- Author of the Oracle Security step-by-step guide and “Oracle Expert Practices”, “Oracle Incident Response and Forensics” books
- **Oracle ACE 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

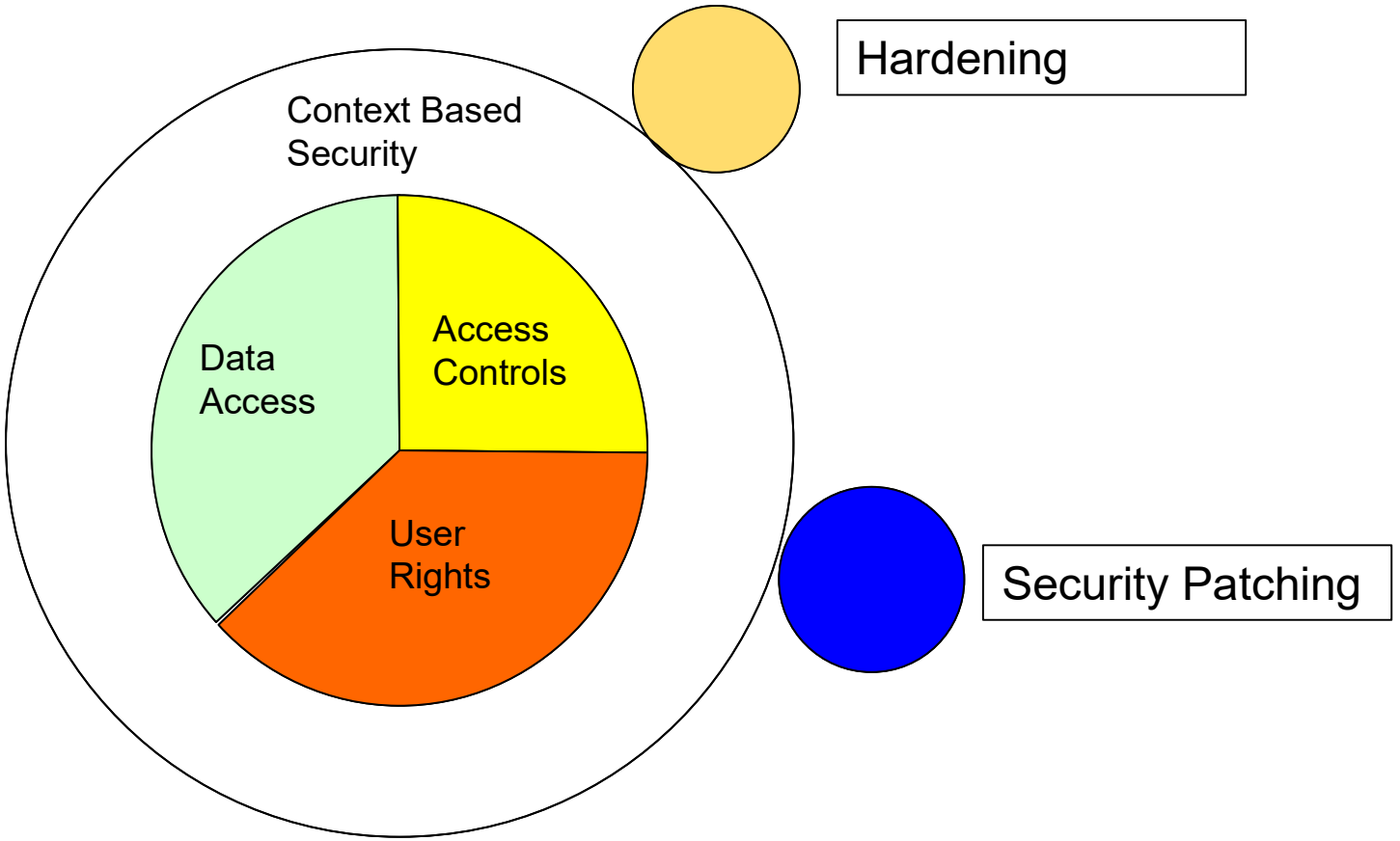
- Securing Oracle
- Where does least privilege fit
- Live demo of reducing the grants of a sample database user
- Where next

PFCL
PETEFINNIGAN.COM LIMITED

# Compartmentalise Data Security?



# The Areas to Secure Data in Oracle Database



PFCL
PETEFINNIGAN.COM LIMITED

# Least Privileges

- For every database user (or schema) they MUST have just the correct rights to allow them to do their job properly and no more
- This is hard to achieve in new databases
- **Even harder in existing databases**
- There is always a fear that something will break
- My experience of performing security audits is the opposite usually exists
  - Most customers end up with MOST PRIVILEGE not LEAST PRIVILEGE

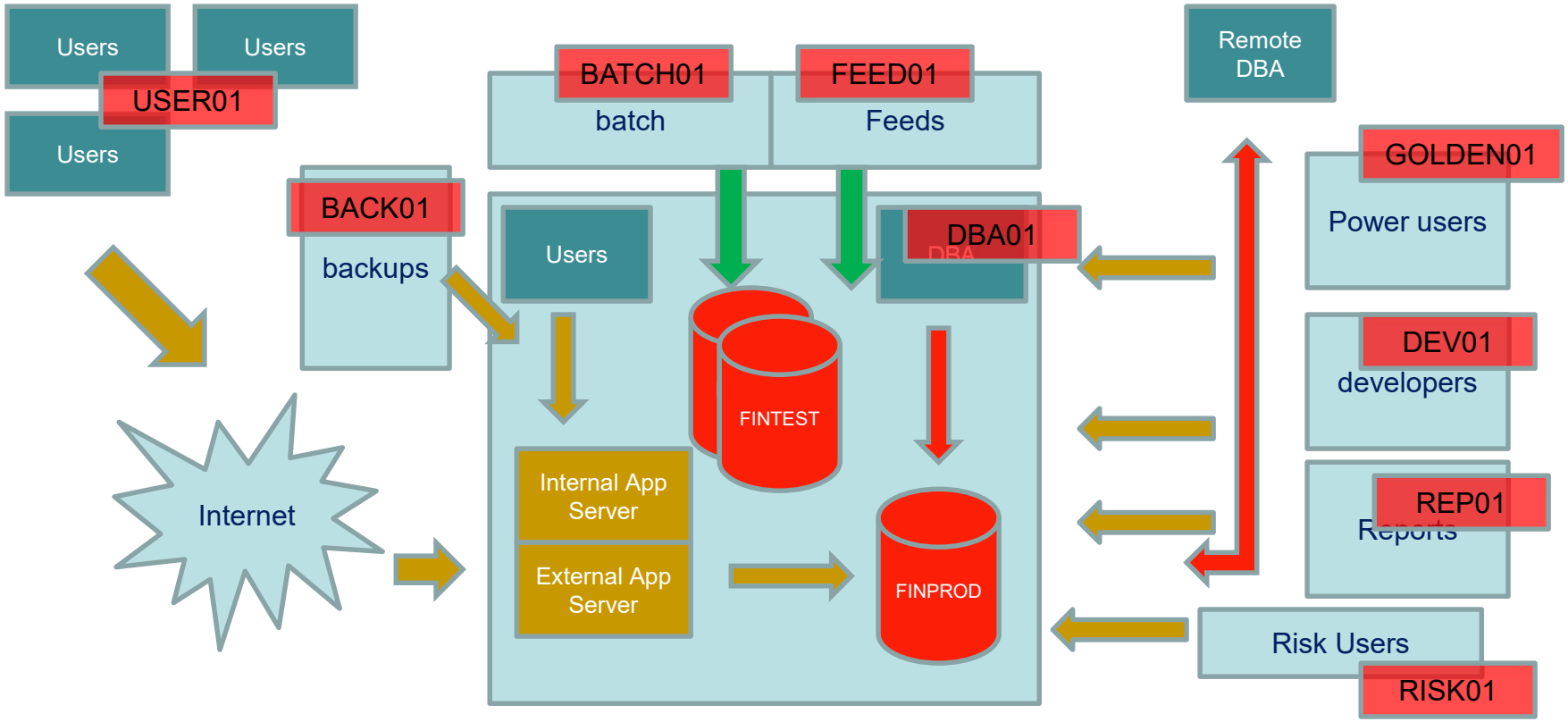
PFCL
PETEFINNIGAN.COM LIMITED

# Actors and Processes

- 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

# Data Architecture

Users need to be identified and can be analysed technically later




# Gather All Users/Roles Privileges

Demo – gather all privileges from the database to use to assess role structure, users rights and also which users have which roles:

- Run jd_f.sql to gather all privileges for all users
- Run jd_r.sql to gather all privileges for all roles
- Run jd_who_has_role.sql to gather all users granted all roles

PFCL
PETEFINNIGAN.COM LIMITED

# Web Based Application – Focus on ORABLOG

BOF: Back Office Customer Management - PeteFinnigan.com Limited

- Address
- Customers
- Employees
- Offices
- Orders
- Order Details
- Payments
- Pay Details
- Person
- Products
- Shipping
- Supplier

## Display Pay Details

number of records found is:2

Add a New Pay Details here

| Id | Amount | Name On Card | Cc34 | Start Date | End Date | Last Four | Edit |
|---|---|---|---|---|---|---|---|
| 1 | 13-MAR-2012 - 2495 | Mr David Bentley | 4049877198543457 | 01-FEB-11 | 01-AUG-16 | 3457 | Edit |
| 2 | 18-AUG-2012 - 3880 | Mr Martin Chisholm | 3742345698766678 | 01-APR-12 | 01-OCT-16 | 6678 | Edit |
| Id | Amount | Name On Card | Cc34 | Start Date | End Date | Last Four | Edit |

Add a New Pay Details here


# Flaws in Least Rights for ORABLOG

- ORABLOG is the schema
- ORABLOG is used to connect Apache to the database
  - **(We will not fix this in this simple demo but should do so later)**
- ORABLOG has two roles from Oracle designed more than 25 years ago – CONNECT and RESOURCE
- ORABLOG needs grants for RUN TIME
- ORABLOG needs grant only at CREATE TIME
- ORABLOG has some small duplication in grants
- ORABLOG has direct grants that can be moved to the roles
- ORABLOG has some sweeping grants such as UNLIMITED TABLESPACE


Demo: orablog.sql

# Demonstration of Privilege Reduction

- First concentrate on the use of Oracle designed roles
  - These are inappropriate for Orablog and BOF application
- Create new ORABLOG roles with the same rights
- Transfer ORABLOG to use these new roles
- Remove privileges to suit the current ORABLOG design and use from these new roles
  - Match roles privileges to objects that exist in the schema
  - Move direct grants to the roles
  - Remove the roles
- Check the direct grants and reduce
- Remove UNLIMITED TABLESPACE and replace with quotas
  - Revoke of RESOURCE will do this in 11.2.0.4 and 12c


This is a hard task and requires a lot of planning, work, testing.

# Further Privilege Analysis

- Focus on removal of these privileges from all users:
  - DBA role and SYSDBA, IMP_FULL_DATABASE, …
  - ALL PRIVILEGES
  - With admin and with grant
  - %ANY%
  - Privileges related to USER, GRANT, ROLE, PROFILE and AUDIT
  - UNLIMITED TABLESPACE
  - CREATE
  - Excessive data access – should be limited to the needs of the application or user


# Consider DBA tasks

- Don't use SYSDBA or SYS
- Don't use the DBA role
- Design your own role
- Create your own accounts for accountability
- Its possible to work day to day with very limited rights
- Who knows what each of more than 200 grants does anyway!
- Use proxy to allow tasks such as:
  - application support,
  - Release and change control


# Conclusions

- Understand the grants made to every user
- Understand what each account is used for (schemas and interactive users)
- Take control of grants
- Don’t use ORACLE roles; they do not match your applications!!
- Remember a DBA does not need all grants all day every day


# User Least Privilege

UKOUG – Liverpool 2018