HROUG-2009

Database Audit and Security

Aci Polajnar acip@mri.si
Uroš Majcen uros.majcen@mri.si

Oracle As a Security Company (A Flavour)

- The name “Oracle” came from a CIA project at Ampex Corp that the authors of Oracle all worked on. Started as SDL (*Simple DirectMedia Layer*) (1977)
- One of the first customers were Wright-Patterson Air Force Base and also the CIA
- Oracle version 2 (1980) included rudimentary passwords
- Oracle 5 added three system privileges, CONNECT, RESOURCE and DBA! – no other privileges could be added
- The “old” password algorithm; DES (*Data Encryption Standard*) based was around from Oracle 6 to Oracle 10gR2
- Oracle version 6 included the concept of roles, three canned roles
- DBA, CONNECT and RESOURCE
- Oracle Advanced networking option was added in Oracle 7.3

Oracle Security Features (A Flavour 2)

Oracle provides (in current versions):

- Users / Schemas
- Roles
- System privileges
- Password and resource management
- Audit features via:
  - Core audit
  - Fine Grained Audit (FGA)
  - Triggers
- Identification and authentication
- Virtual Private Database (VPD) => Also Oracle Label Security (OLS)
- Built-in encryption – for database and file system (Transparent Data Encryption)(TDE)
- Network encryption solutions

What’s Gone Wrong With Database Security ?

Anyone?

What’s Gone Wrong ?

- The rise of the internet and networked applications
- A recent realisation that network security doesn’t protect an Oracle database. The applications after all tunnel SQL to the database through firewalls!
- Recent need to protect data and particularly financial data such as credit cards or personally identifiable data
- Legislation and regulations are now prevalent in a lot of market sectors
- Most database installations are default with no attempt at hardening
- Oracle don’t make it easy to secure Oracle as they provide an “open” installation by default – all functions and features are available to almost all users
- Finally the insider threat is more real than the external threat

The Place Of The Database In Security

- The database, the Oracle database is central to most businesses that use and process data
- Often the business data and processes are driven from the Oracle database
- Global and networked business makes the Oracle database accessible to a much wider audience
- Key data such as financials, personally identifiable data, business data, client lists, HR data and more are stored and processed in and with an Oracle database
- The Oracle database has become central to organisations security plans. Unfortunately most companies have not moved towards securing the Database
- Most security firms concentrate on network security and take a cursory look at Oracle

Patches – Older Ones and CPU’s (Critical Patch Update)

- A major issue plaguing Oracle customers is the “to patch or not to patch” issue
- There is a trend across most Oracle customers to not apply security patches, to run on old versions or unsupported patch sets of the database software
- Whilst this is a major issue that Oracle must help solve its only part of the securing Oracle story
- It is only part of securing Oracle and what we are learning on the courses
- CPU’s are extremely important but don’t make them the end goal

Exploits

- Oracle has fixed an unprecedented number of security bugs (hundreds)
- Each Critical Patch Update (CPU) fixes large numbers of database security bugs
- Each CPU often is followed closely by exploit code published to sites such as http://www.milw0rm.com
- Oracle also silently fix bugs in each CPU – these are not listed in the advisories
- A number of commercial companies and researchers reverse engineer the patches to find and write exploits
- Because of the nature of most exploits there are an infinite number of possible exploits that can be written
- Different payloads, Intrusion detection system (IDS) evasion techniques and more

Key Security Concerns

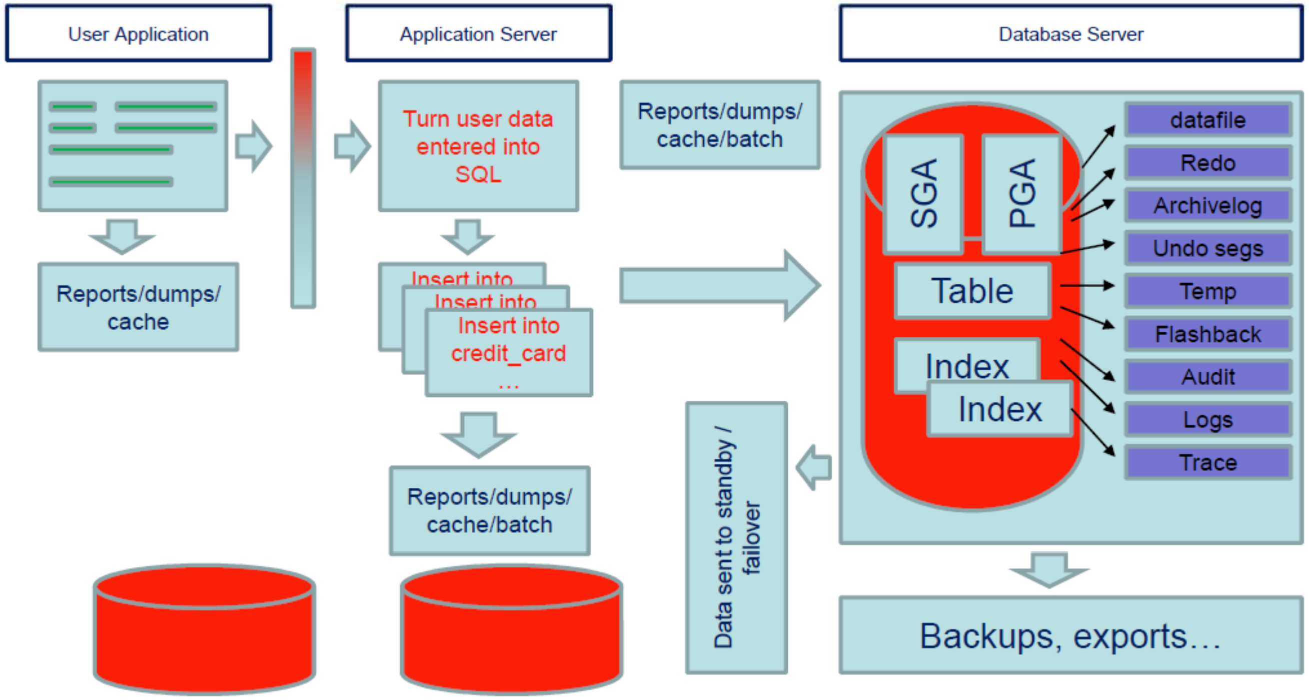
The core issues with Oracle database security are:

- Wrong products installed – EE when SE would do
- Default installations – too many software features installed
- Default schemas installed – a fault of a default install
- Passwords weak – defaults, pwd=user, dictionary words, too short
- No audit enabled
- Default configurations in place
- Bad user privilege design – not least privilege principal
- DBA’s use SYS and SYSTEM and share accounts
- The database can be accessed from anywhere using TNS
- Much more…..

Where Is The Data?

It’s in a database table, right?

Where Is The Data?



User Application

Application Server

Database Server

Turn user data entered into SQL

Reports/dumps/ cache/batch

Reports/dumps/ cache

Insert into

Insert into

Insert into credit_card …

Reports/dumps/ cache/batch

SGA

PGA

Table

Index

Index

datafile

Redo

Archivelog

Undo segs

Temp

Flashback

Audit

Logs

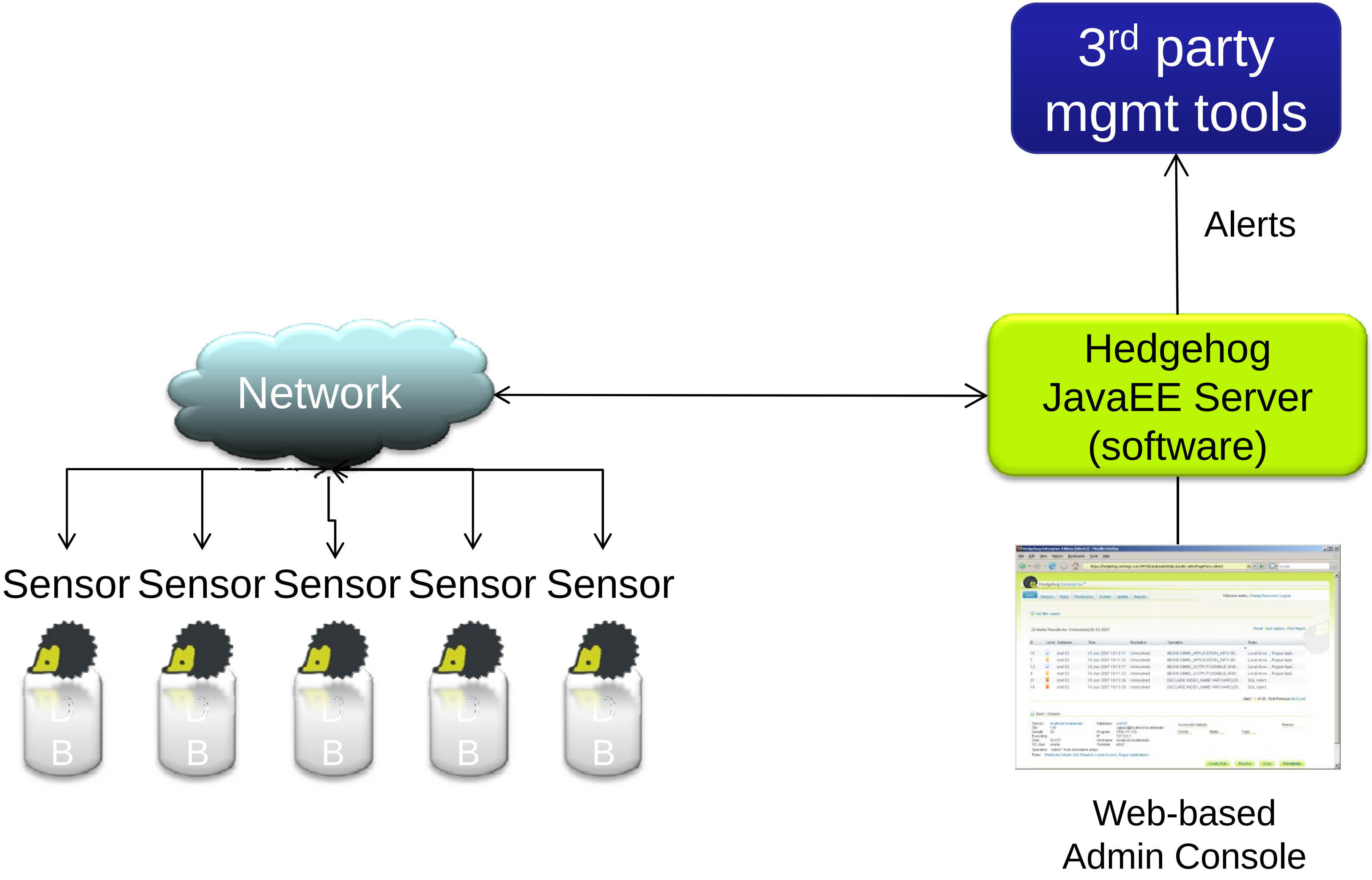
Trace

Data sent to standby / failover

Backups, exports…

36

Hedgehog: Architecture Overview



3rd party mgmt tools

Alerts

Hedgehog JavaEE Server (software)

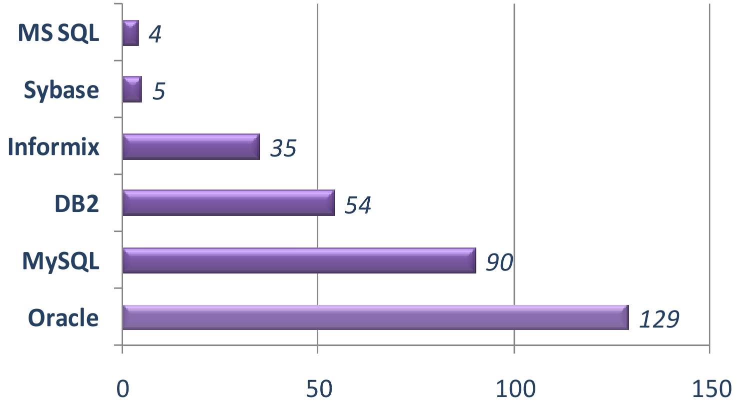
Network

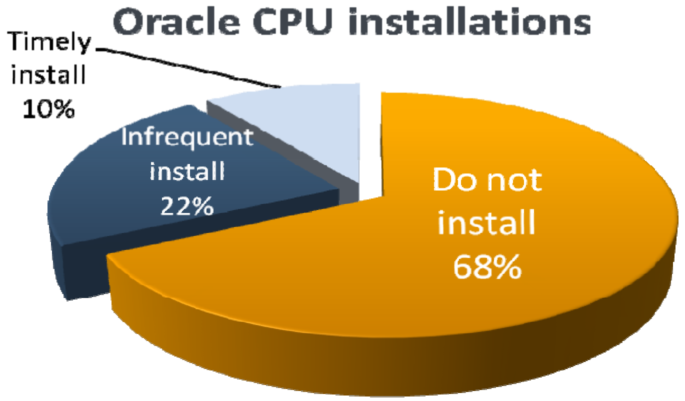
Sensor Sensor Sensor Sensor Sensor

Web-based Admin Console

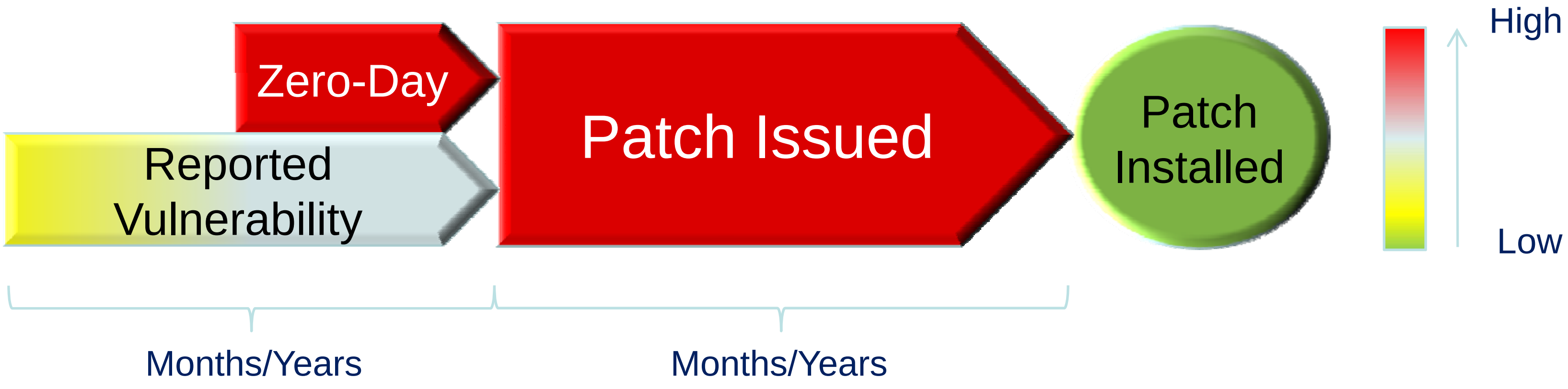
Oracle security patches (CPUs)

- More than 100 severe vulnerabilities open at any point in time
- Users do not patch their databases:
  - Application providers advise their customers not to install the Orcle CPUs
  - DB must be taken down, application should be thoroughly tested





The Risk Window is Significant



- Exploits published on the web
  - Zero-days (before the patch)
  - Within days after a patch is issued
  - Often do not require DBA-level skill
- Risk window is months long, sometimes years long
- Risk highest *after* patch is issued

Advantages of **Hedgehog vPatch**

- **No business interruption**
  - Initial installation and implementation take hours
  - Ongoing operation is transparent (like anti-virus)
  - No need to take DB down
  - No impact on the application
- **Immediate protection**
  - It's faster to vPatch than to patch
- **Zero day coverage**
  - Generic, context based protection
- **Coverage for unsupported Oracle versions: 8i, 9i**
  - 40% - 50% of Oracle users are still using these versions

Repscan – By Red-Database-Security

Available exclusively trough www.sentrigo.com

- Detects insecure PL/SQL-Code
- Shows the patch level of all your databases in one-click
- Finds security problems such as SQL Injections, hardcoded passwords, deprecated functions
- Detects weak or default passwords
- More than 115 Oracle tables checked for password information
- Provides penetration testing reports
- Detects changed database objects including root kits
- Detects altered data (including modifications of privilege and user tables)
- Discovers forensic traces from common security and hacker tools
- Complements and integrates with Sentrigo's Hedgehog family of database activity monitoring software

Thank you

Aci Polajnar acip@mri.si

Uroš Majcen uros.majcen@mri.si