

Ghost Data & Spectral Data - When is Encrypted Data Not Encrypted? And when is your data in places you didn't expect



Jonathan Intner
J. S. Intner, Consulting, LLC
16 September, 2009

Agenda



- ✧ Introduction
- ✧ Background
 - ✧ Why encrypt?
 - ✧ Definitions
 - ✧ Problem Statement
- ✧ Test Cases:
 - ✧ Conceptually
 - ✧ 11g: tablespace
 - ✧ 10g: column

Introduction



- ✦ DBA for more than 20 years
- ✦ Certifiable:
 - ✦ OCP
 - ✦ Computer Information Systems Security Professional (CISSP)
- ✦ Currently, Project Manager and Database Architect on a Global Oracle Upgrade Project

Why Encrypt?



- ✧ Data Breach Regulations:
 - ✧ GLBA, SOX, Ca SB1386, HIPAA, PCI-DSS, EC 45/2001 & EC Decision No 1247/2002/EC, etc.
- ✧ These breaches do occur:
 - ✧ See <http://www.privacyrights.org/ar/ChronDataBreaches.htm>
- ✧ And they have a real cost:
 - ✧ Loss of reputation
 - ✧ Increased monitoring requirements and regulatory penalties
 - ✧ Outright cost of \$90 to \$305 per record

Definitions (1)



- ✦ Encryption
- ✦ Wallet
- ✦ Oracle's Advanced Security Option (ASO)
 - ✦ Transparent Data Encryption (TDE)

Definitions (2)



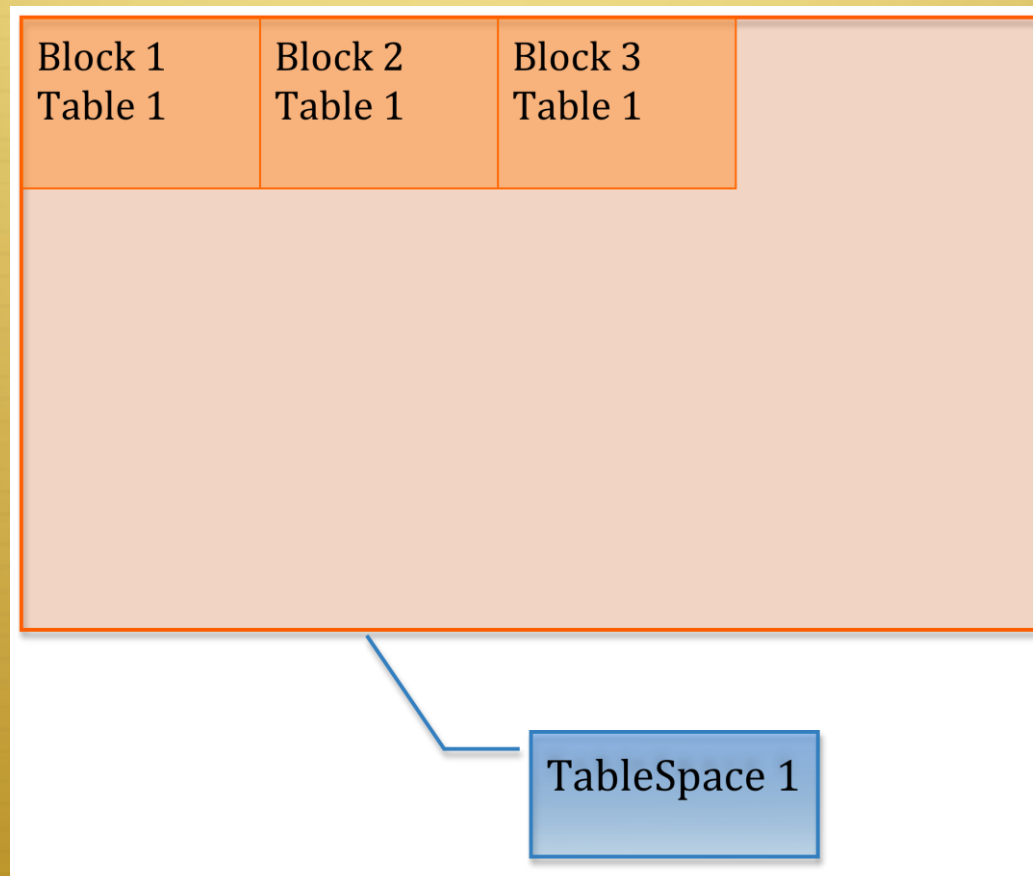
✧ Ghost Data:

- ✧ http://www.oracle.com/technology/deploy/security/database-security/transparent-data-encryption/tde_faq.html#A15032

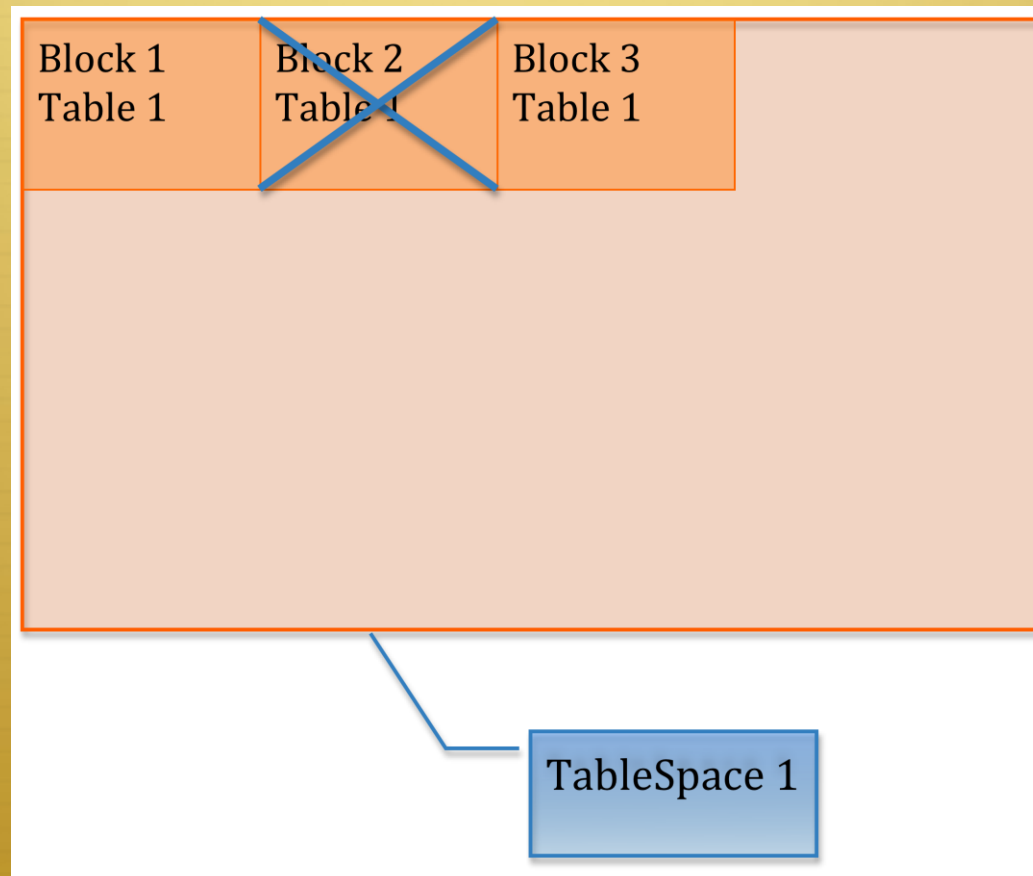
✧ Spectral Data

- ✧ Spectral data is a variant on Ghost Data, except data from one tablespace can end up in another!
- ✧ More available at:
<http://www.freelists.org/post/oracle-1/Ghost-Data>

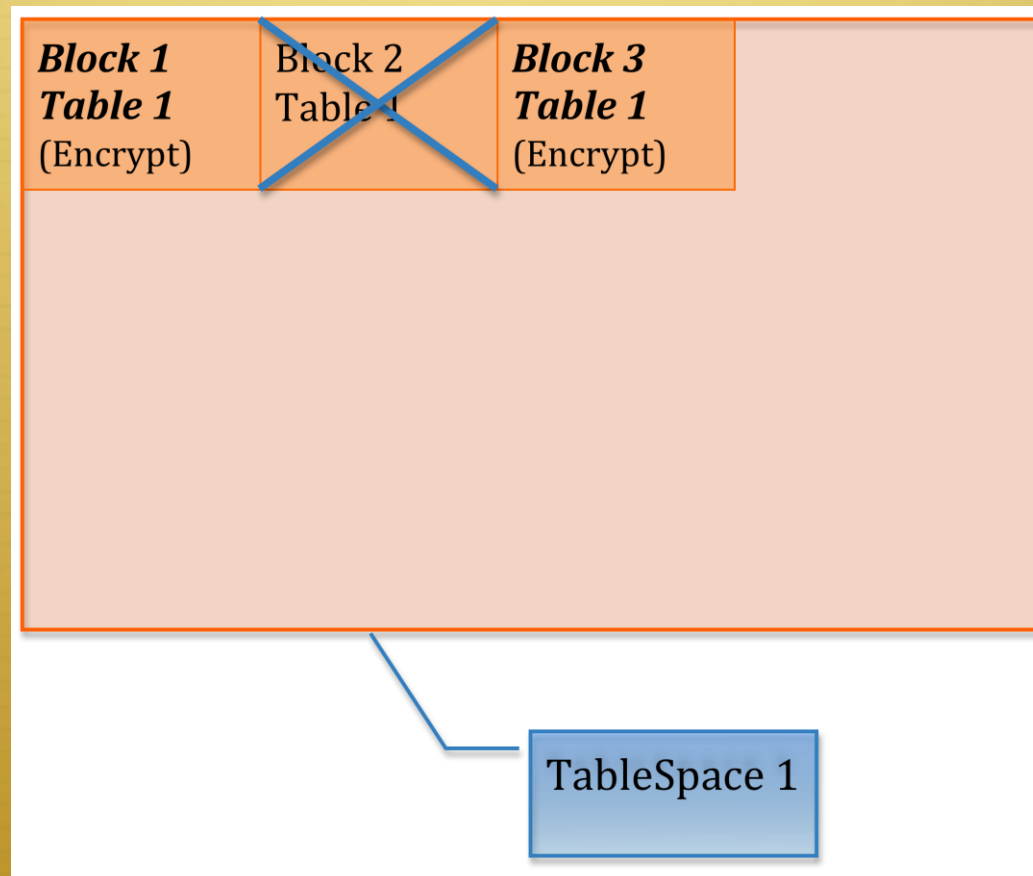
Ghost Data Diagram



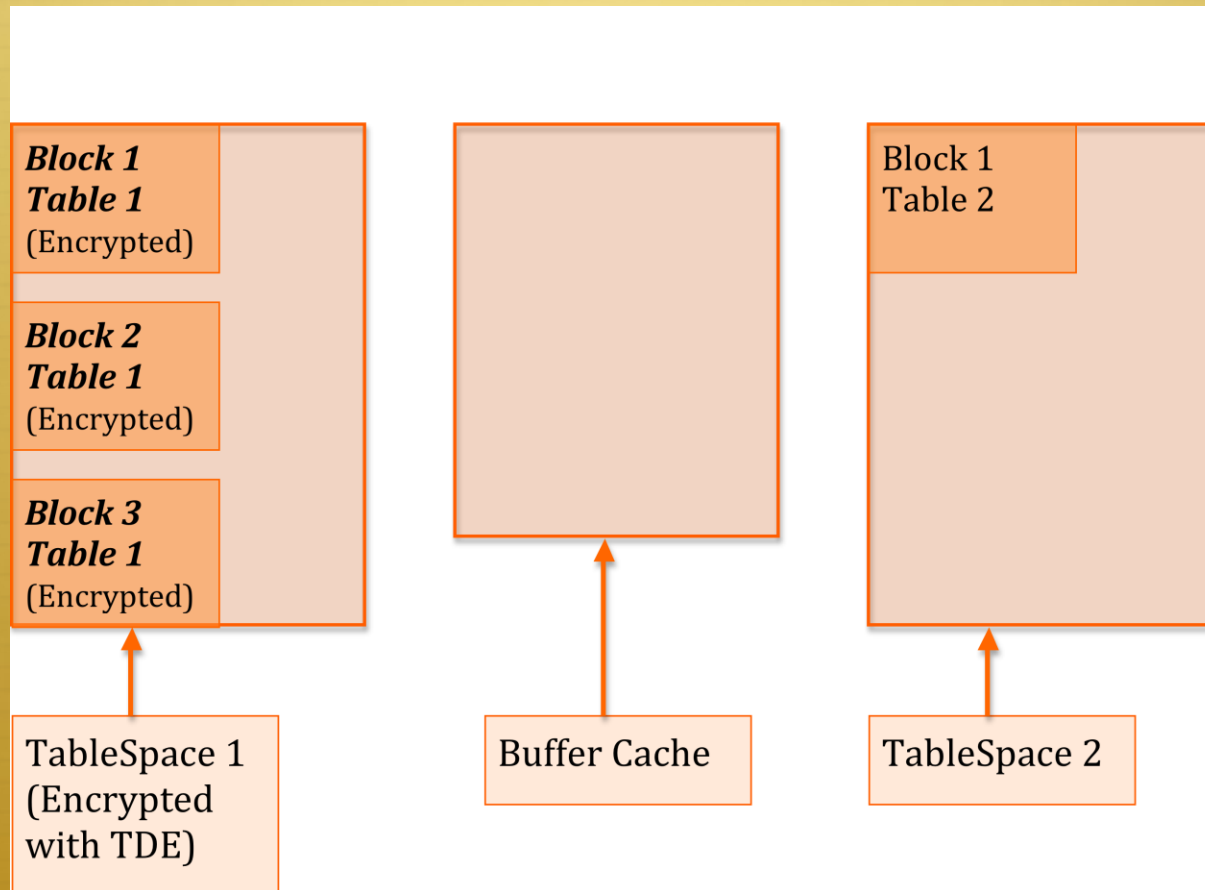
Ghost Data Diagram



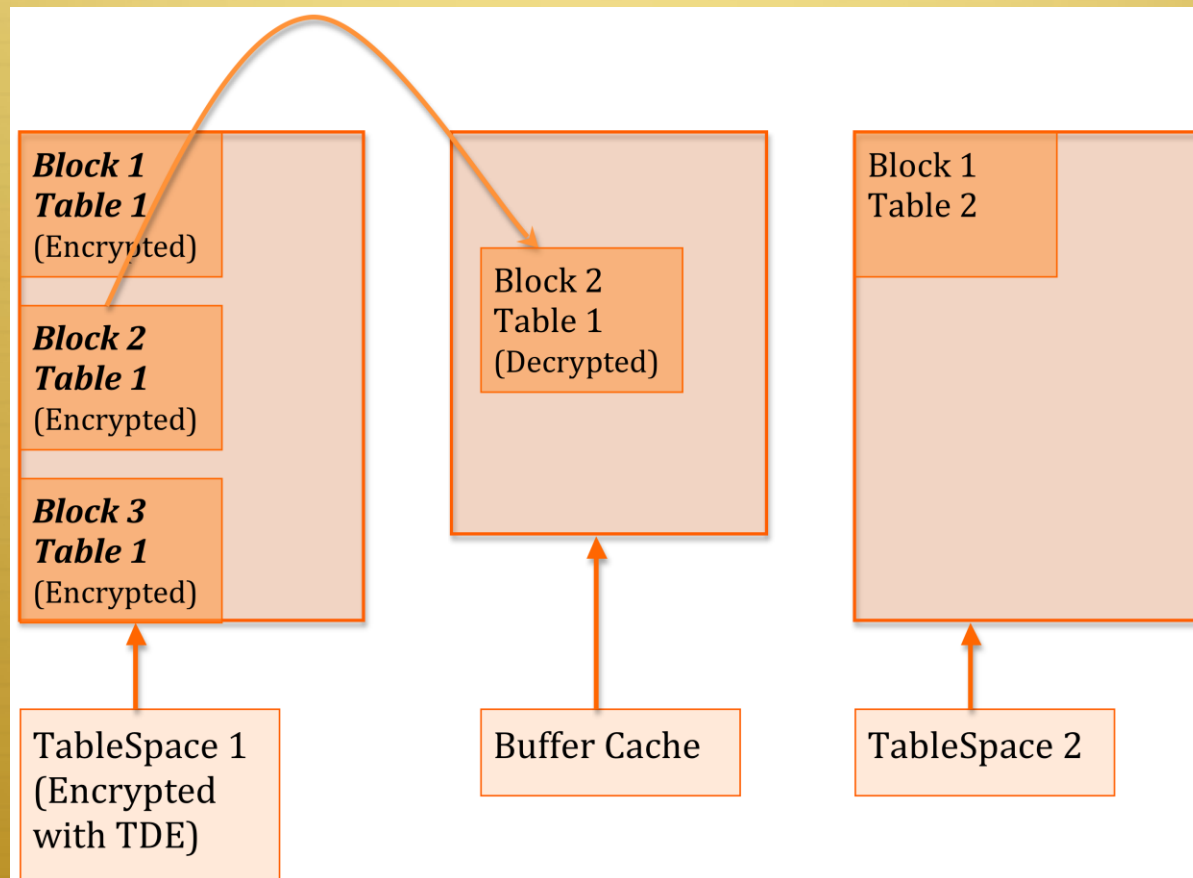
Ghost Data Diagram



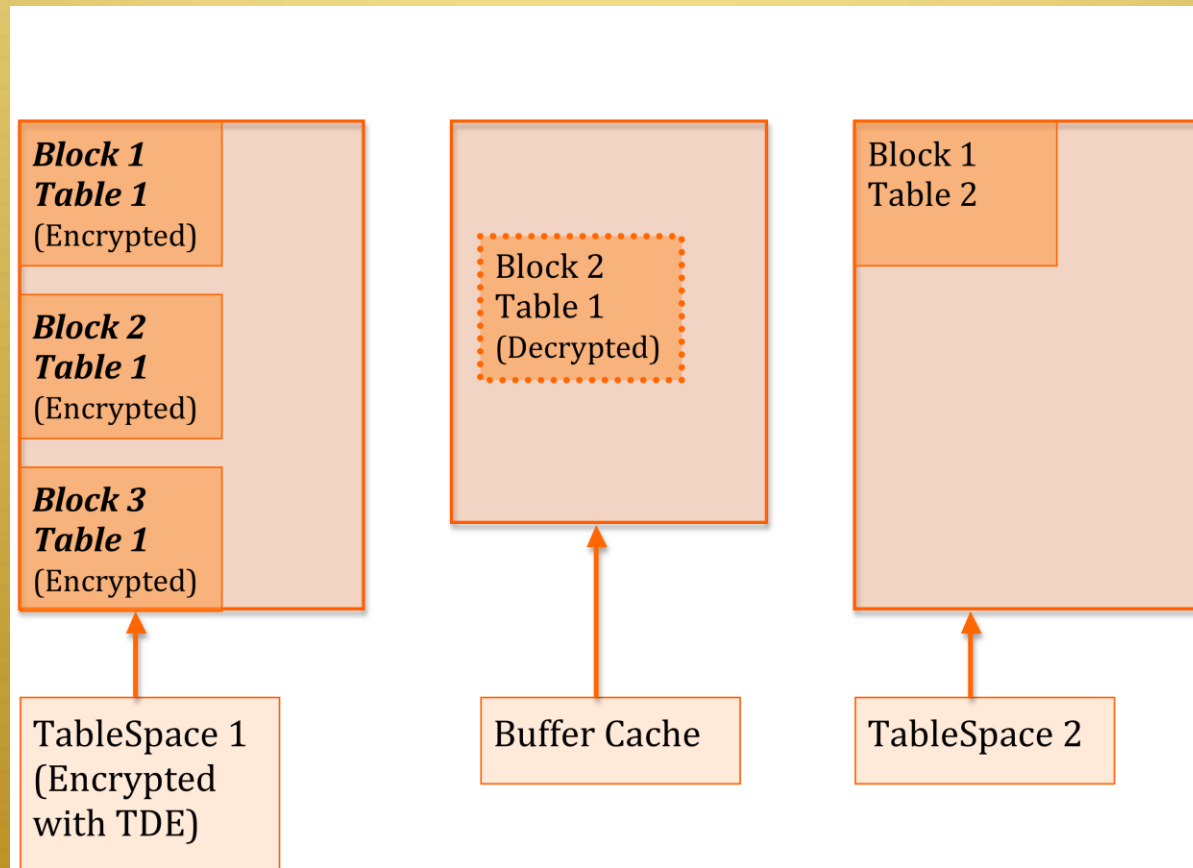
Spectral Data Diagram



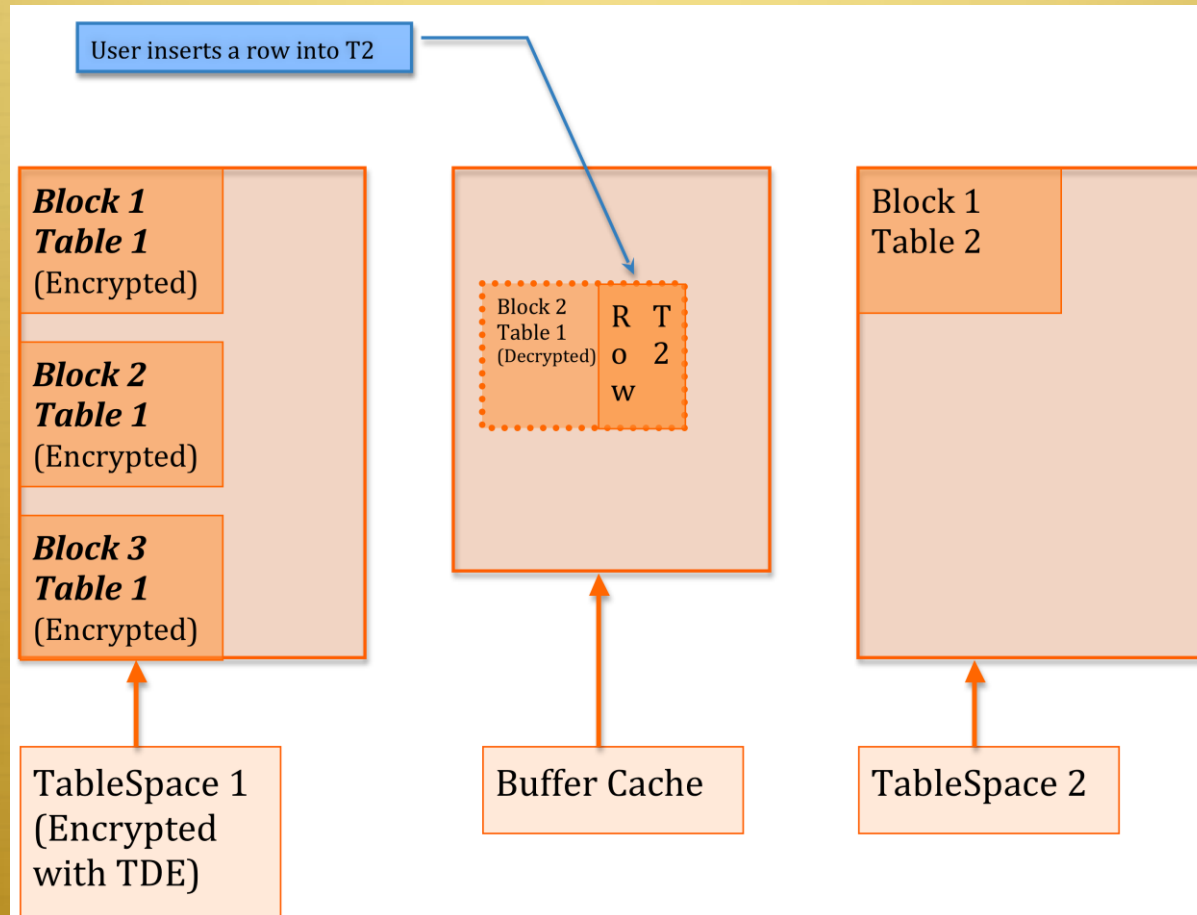
Spectral Data Diagram



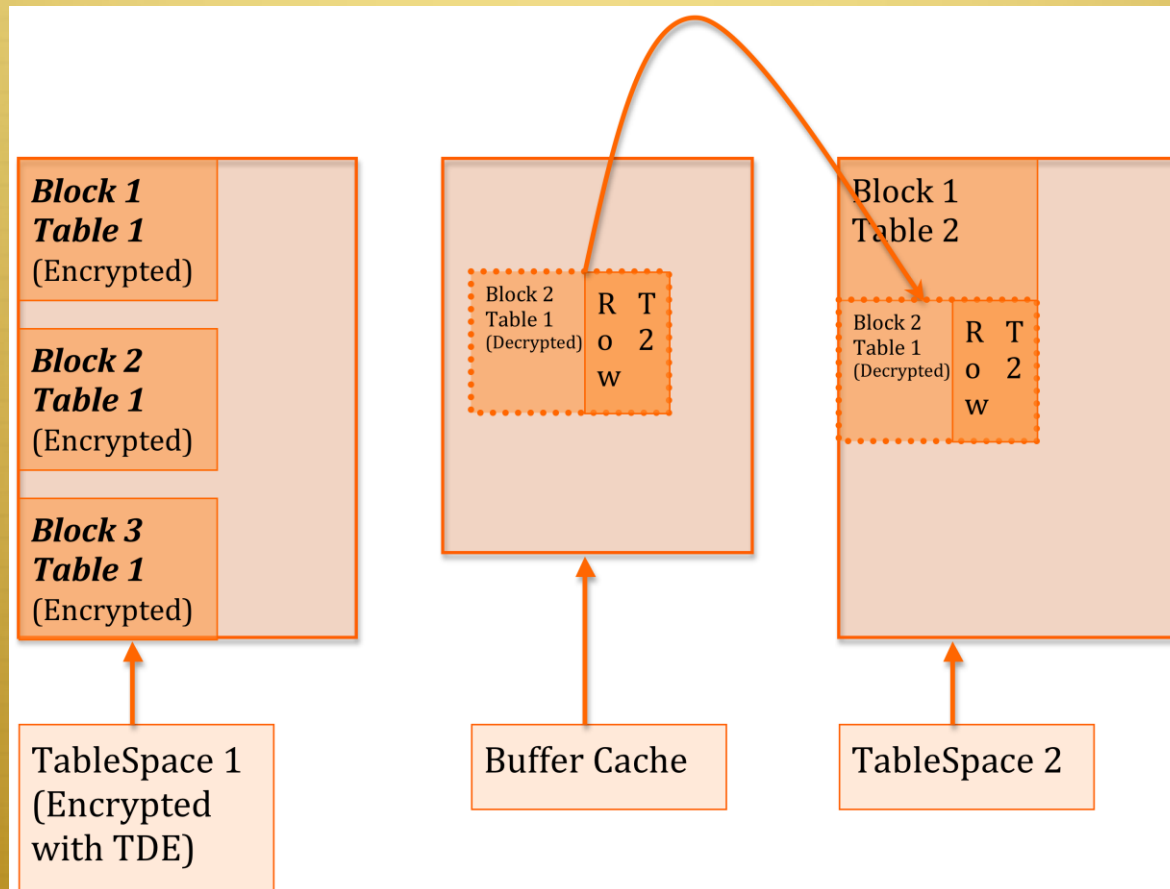
Spectral Data Diagram



Spectral Data Diagram



Spectral Data Diagram



Test Case: Conceptual



- ✦ Install Oracle:
 - ✦ 11.1.0.7 with the July 2009 Critical Patch Update
 - ✦ 10.2.0.4 with the July 2009 Patch Set Update
- ✦ Shrink the buffer cache, so a single table can fill its blocks.
- ✦ Create encrypted data.
- ✦ Fully populate the buffer cache with this encrypted data.
- ✦ Insert a row into an unencrypted data and, if you used 11g's tablespace-encryption that is available with TDE, you'll see your encrypted data, decrypted.
 - ✦ Different behavior with column-level TDE data caused me to realize there's a corollary: EVERY TIME A ROW IS INSERTED FROM A PARTIALLY-FULL BLOCK IN THE BUFFER CACHE, YOU END UP WITH "SPECTRAL" DATA IN A TABLESPACE!

Commands (1)



- ✦ Shrink the SGA & Buffer Cache.
- ✦ Enable TDE:
 - ✦ Be careful where your wallet ends up.
 - ✦ The command is:
 - ✦ ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY password;
 - ✦ Use Oracle Wallet Manager (run by typing “owm” on *nix) to manage the wallet.

Commands (2)



- ✦ Configure SQLNET.ORA for the location for the Wallet.
- ✦ Command to add:
encryption_wallet_location =
 (source =
 (method = file
 (method_data =
 (directory = <your choice>)))
- ✦ With 11g, it should be possible to use other locations, like an external device.

Commands (3)



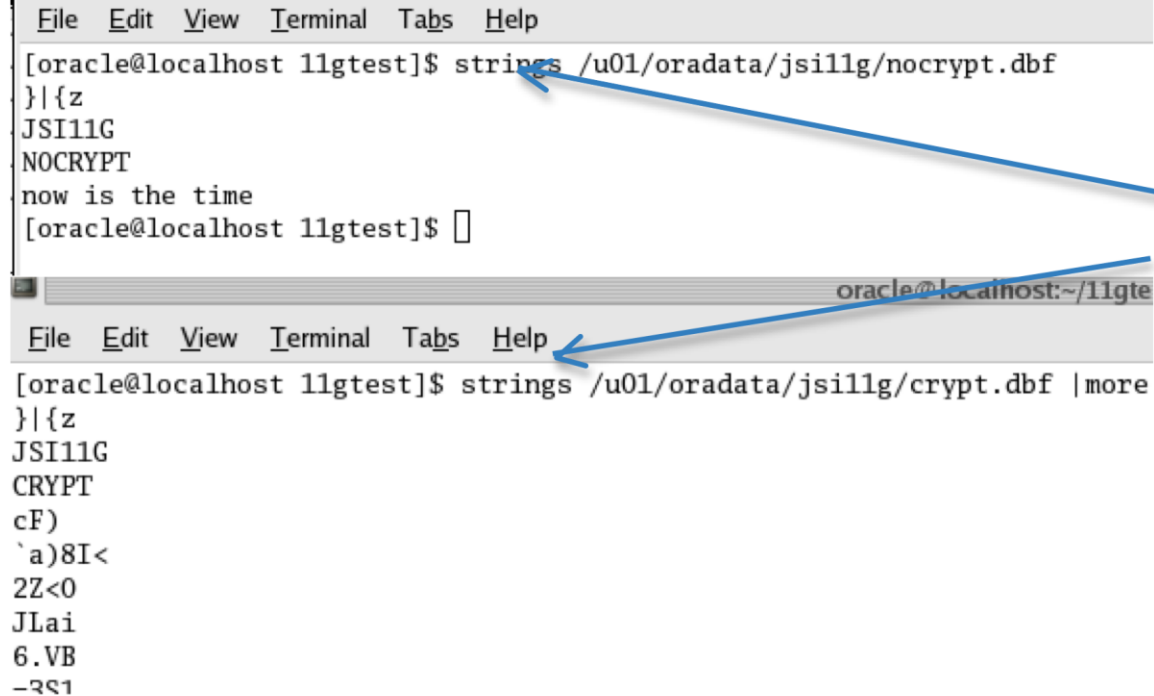
- ✧ Wallet opened after DB re-started:
 - ✧ ALTER SYSTEM SET ENCRYPTION WALLET OPEN IDENTIFIED BY "password";
- ✧ Create an encrypted tablespace:
 - ✧ create tablespace fred
datafile '/u01/app/oracle/oradata/phmupg2/fred.dbf'
size 100m encryption using '3des168'
default storage (encrypt);

Commands (4)



- ✧ Used the following commands to load data into a table in that tablespace:
 - ✧ `create table foo tablespace fred as
select * from dba_objects;`
 - ✧ `-- execute the following until the tablespace fills:`
 - ✧ `insert into foo (select * from foo);`

Tablespaces

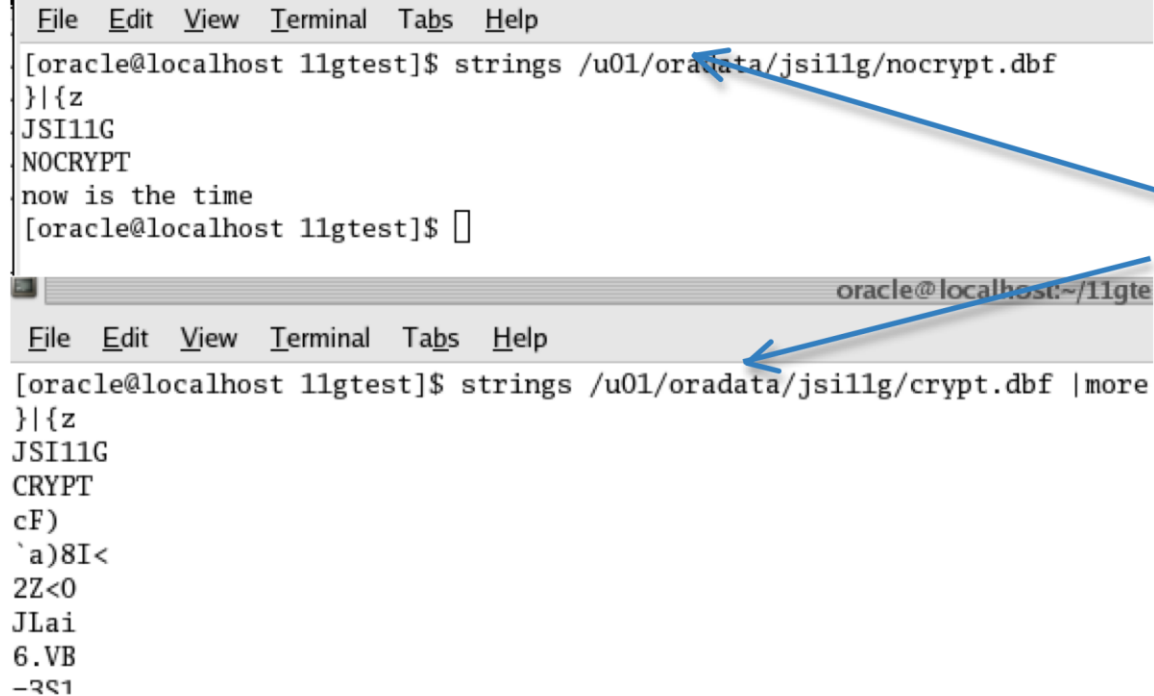


```
File Edit View Terminal Tabs Help
[oracle@localhost 11gtest]$ strings /u01/oradata/js111g/nocrypt.dbf
}|{z
JSI11G
NOCRYPT
now is the time
[oracle@localhost 11gtest]$

oracle@localhost:~/11gte
File Edit View Terminal Tabs Help
[oracle@localhost 11gtest]$ strings /u01/oradata/js111g/crypt.dbf |more
}|{z
JSI11G
CRYPT
cF)
`a)8I<
2Z<0
JLai
6.VB
-391
```

OS Command

Tablespaces



```
File Edit View Terminal Tabs Help
[oracle@localhost 11gtest]$ strings /u01/oradata/js11g/nocrypt.dbf
}|{z
JSI11G
NOCRYPT
now is the time
[oracle@localhost 11gtest]$

oracle@localhost:~/11gte
File Edit View Terminal Tabs Help
[oracle@localhost 11gtest]$ strings /u01/oradata/js11g/crypt.dbf |more
}|{z
JSI11G
CRYPT
cF)
`a)8I<
2Z<0
JLai
6.VB
-391
```

Files

Tablespaces

File Edit View Terminal Tabs Help

```
[oracle@localhost 11gtest]$ strings /u01/oradata/jsi11g/nocrypt.dbf
```

```
}|{z
```

```
JSI11G
```

```
NOCRYPT
```

```
now is the time
```

```
[oracle@localhost 11gtest]$
```

DB/TS Names

oracle@localhost:~/11gte

File Edit View Terminal Tabs Help

```
[oracle@localhost 11gtest]$ strings /u01/oradata/jsi11g/crypt.dbf |more
```

```
}|{z
```

```
JSI11G
```

```
CRYPT
```

```
cF)
```

```
`a)8I<
```

```
2Z<0
```

```
JLai
```

```
6.VB
```

```
-391
```

Tablespaces

File Edit View Terminal Tabs Help

```
[oracle@localhost 11gtest]$ strings /u01/oradata/jsi11g/nocrypt.dbf  
}|{z  
JSI11G  
NOCRYPT  
now is the time  
[oracle@localhost 11gtest]$
```

Plain Text
Data

File Edit View Terminal Tabs Help

```
[oracle@localhost 11gtest]$ strings /u01/oradata/jsi11g/crypt.dbf |more  
}|{z  
JSI11G  
CRYPT  
cF)  
'a)8I<  
2Z<0  
JLai  
6.VB  
-391
```

Encrypted
Data

Create the problem



- ✦ Fully populate the buffer cache with data from the encrypted tablespace.
- ✦ Create a shell script that contains repeated executions of the following:

```
sqlplus /nolog << EOF
connect / as sysdba
select * from foo;
exit
EOF
```
- ✦ While the above shell script is running, insert a row into the table in the unencrypted tablespace and examine the datafile for that tablespace with the Unix “strings” command. This confirms that unencrypted data was written to disk.

De-crypted, Encrypted data in decrypted tablespace

The image consists of two terminal windows. The top window shows a search for specific data in a database. The bottom window shows the same data retrieved from a decrypted tablespace file.

Top Terminal Window:

```
oracle@localhost:~/11gtest
File Edit View Terminal Tabs Help
[oracle@localhost 11gtest]$ egrep '/f8a912ac_PowerPCAbstractMIR2L|/20ad55b7_PowerPCAbstractMIR2L|/20ad55b7_PowerPCAbstractMIR2L|/1d5fe4c_PowerPCAbstractMIR2LI|/1d5fe4c_PowerPCAbstractMIR2LI|/f3d38a64_PowerPCAbstractMIR2L|/f3d38a64_PowerPCAbstractMIR2L' nohup.out | sort -u
PUBLIC          /1d5fe4c_PowerPCAbstractMIR2LI
PUBLIC          /20ad55b7_PowerPCAbstractMIR2L
PUBLIC          /f3d38a64_PowerPCAbstractMIR2L
PUBLIC          /f8a912ac_PowerPCAbstractMIR2L
SYS             /1d5fe4c_PowerPCAbstractMIR2LI
SYS             /20ad55b7_PowerPCAbstractMIR2L
SYS             /f3d38a64_PowerPCAbstractMIR2L
SYS             /f8a912ac_PowerPCAbstractMIR2L
[oracle@localhost 11gtest]$
```

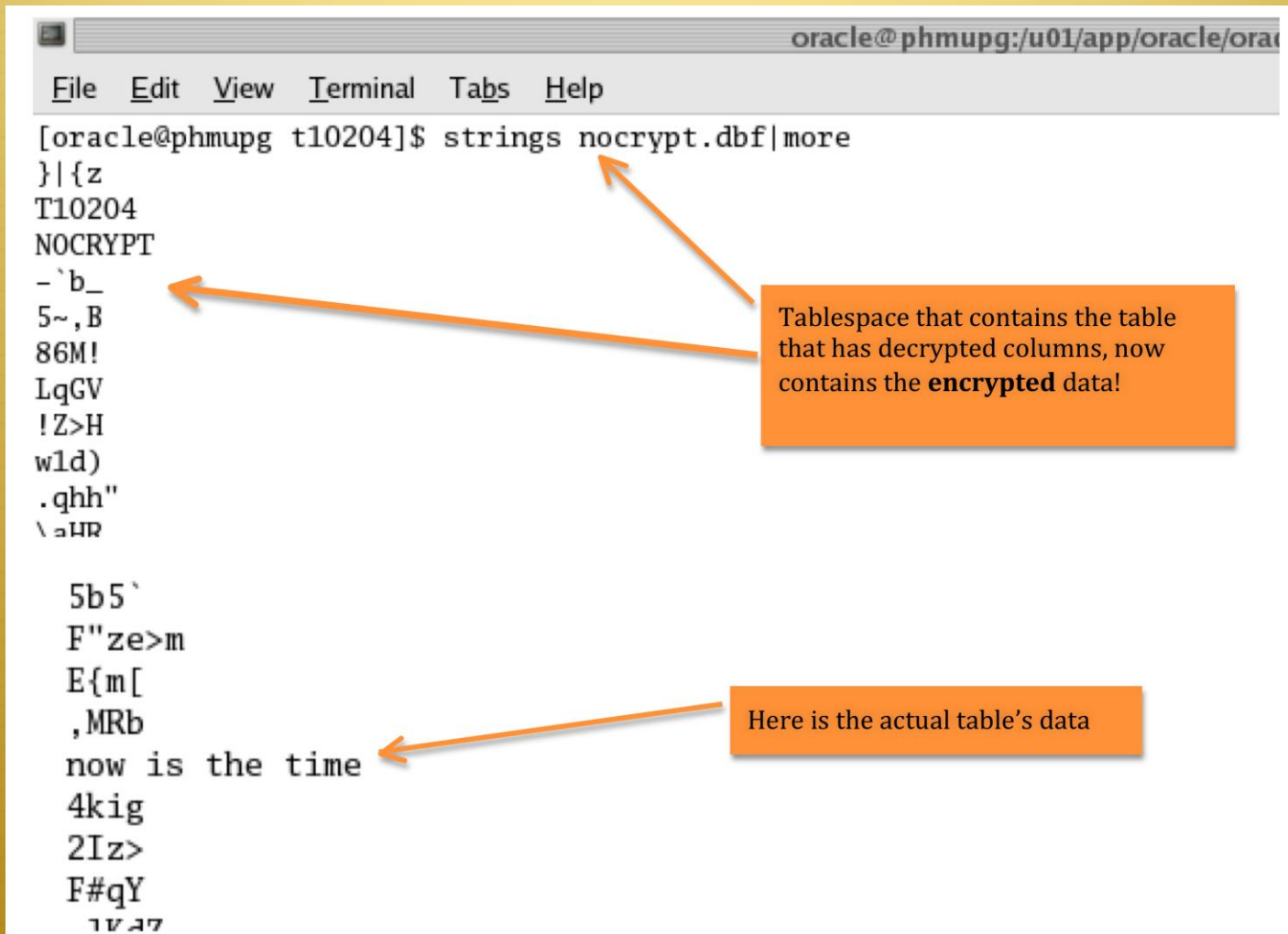
Bottom Terminal Window:

```
oracle@localhost:~/11gtest
File Edit View Terminal Tabs Help
[oracle@localhost 11gtest]$ strings /u01/oradata/js111g/nocrypt.dbf | more
}|{z
JSI11G
NOCRYPT
p      P      @      0
128"
o%<"
1X^
now is the time
/f8a912ac_PowerPCAbstractMIR2L
/20ad55b7_PowerPCAbstractMIR2L
/20ad55b7_PowerPCAbstractMIR2L
/1d5fe4c_PowerPCAbstractMIR2LI
/1d5fe4c_PowerPCAbstractMIR2LI
/f3d38a64_PowerPCAbstractMIR2L
/f3d38a64_PowerPCAbstractMIR2L
[oracle@localhost 11gtest]$
```

Annotations:

- Searching result set:** A box pointing to the search results in the top terminal window.
- Decrypted Tablespace:** A box pointing to the output of the `strings` command in the bottom terminal window.
- Same Content:** A label with an arrow pointing from the search results in the top window to the output in the bottom window, indicating that the data is identical.

Column Encryption



```
oracle@phmupg:/u01/app/oracle/ora
File Edit View Terminal Tabs Help
[oracle@phmupg t10204]$ strings nocrypt.dbf|more
}|{z
T10204
NOCRYPT
-`b_
5~,B
86M!
LqGV
!Z>H
wld)
.qhh"
\ aUR

5b5`
F"ze>m
E{m[
,MRb
now is the time
4kig
2Iz>
F#qY
1V 27
```

Tablespace that contains the table that has decrypted columns, now contains the **encrypted** data!

Here is the actual table's data

Closing



- ✦ I understand that Oracle does consider this behavior a bug and it will be fixed in an upcoming CPU.

References



- ✧ Cost of a data breach:
 - ✧ According to a 2007 study by Forrester Research. Forrester, which notes that estimating the cost of breaches is an inexact science, based its figures on a survey of 28 companies who had some sort of data breach. The costs included legal fees, call center costs, lost employee productivity, regulatory fines, loss of investor confidence and customer losses to estimate these figures. This information and the previous 3 bullets were retrieved from http://www.sans.org/reading_room/analysts_program/DLL_April08.pdf on April 22, 2009.
 - ✧ List of data breaches, including the one referenced on slide 4, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>