Oracle Forensics

Dissection of an Oracle Attack
(Talk and Demo)

David Litchfield
(davidl@ngssoftware.com)
Note to reader:

- These slides were compiled on 29th June 2007
- They’re liable to change from now ‘til when I give the presentation
- Cheers! David
Why Oracle Forensics?

- Since the state of California passed the Database Security Breach Notification Act (SB 1386) in 2003 another 34 states have passed similar legislation with more set to follow.
- In January 2007 TJX announced they had suffered a database security breach with 45.6 million credits card details stolen – the largest known breach so far.
- In 2006 there were 335 publicized breaches in the U.S.; in 2005 there were 116 publicized breaches; between 1st January and March 31st of 2007, a 90 day period, there have been 85 breaches publicized.
- There are 0 (zero) database-specific forensic analysis and incident response tools on the market – free or commercial.
Where is the evidence?

- Evidence of a compromise can be found in many places
  - TNS Log files
  - Trace files
  - Redo Logs
  - Datafiles
  - Apache logs (Oracle Application Server)
- This talk and demo specifically covers the datafiles, redo logs and Apache logs.
- In the essence of time we’ll be cutting out several parts of the forensic process which you wouldn’t do in a real scenario of course!
- To start with we’ll look at an Oracle Data Block
Oracle Data Block

- Header
  - Object ID (25th Byte)
  - Checksum
- Row Directory
  - Each row has 2 byte entry pointing to offset
Oracle Data Block…row of data

Consists of a 3 byte Row Header

Byte 1: Flags to indicate row state

  If row of data has been deleted the 5\textsuperscript{th} bit of 1\textsuperscript{st} byte (Flags) is set – e.g. 0x2C becomes 0x3C

Byte 2: Lock Status

Byte 3: Number of columns
Oracle Data Block...row of data

189d3790h: 2C 01 11
189d37a0h: 04 C3 06 13 2F 04 C3 06 13 2F 02 C1 37 0D 4D 59
189d37b0h: 5F 54 45 4D 50 5F 54 41 42 4C 45 02 C1 02 FF 02
189d37c0h: C1 03 07 78 6B 03 17 12 08 38 07 78 6B 03 17 12
189d37d0h: 08 38 07 78 6B 03 17 12 08 38 07 78 6B 03 17 12
189d37e0h: 80 FF 02 C1 07 02 C1 02
**Oracle Data Block…row of data**

| Col 1 |   | Col 2 |   | Col 3 |   | Col 4 |   | Col 5 |   | Col 6 |   | Col 7 |   | Col 8 |   | Col 9 |   | Col 10 |   | Col 11 |   | Col 12 |   | Col 13 |   | Col 14 |   | Col 15 |   | Col 16 |   | Col 17 |   |
|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|
| 04 C3 06 13 2F |   | 04 C3 06 13 2F |   | 02 C1 37 |   | 0D 4D 59 5F 54 45 4D 50 5F 54 41 42 4C 45 |   | 02 C1 02 |   | FF |   | 02 C1 03 |   | 07 78 6B 03 17 12 08 38 |   | 07 78 6B 03 17 12 08 38 |   | 07 78 6B 03 17 12 08 38 |   | 02 C1 02 |   | FF |   | FF |   | 01 80 |   | FF |   | 02 C1 07 |   | 02 C1 02 |   |
Oracle Data Block... row of data

04 C3 06 13 2F = ((6-1)*10000) + ((19-1)*100) + (47-1) = 51846
04 C3 06 13 2F = ((6-1)*10000) + ((19-1)*100) + (47-1) = 51846
02 C1 37 = 55
0D 4D 59 5F 54 45 4D 50 5F 54 41 42 4C 45 = MY_TEMP_TABLE
02 C1 02 = 1
FF = NULL
02 C1 03 = 2
07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:55
07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:55
07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:55
02 C1 02 = 1
FF = NULL
FF = NULL
01 80 = 0
FF = NULL
02 C1 07 = 6
02 C1 02 = 1
Locating Dropped Objects

To locate dropped objects we need to know what happens when an object is created:

- A row is entered in the OBJ$ table, I_OBJ1, I_OBJ2, I_OBJ3 indexes
- Depending upon object
  TAB$, COL$ for table objects
  SOURCE$, IDL_UB1$, IDL_CHAR$ for functions
- Information about new objects scattered all over the datafile.
Locating Dropped Objects

Open datafile that has the SYSTEM tablespace
Locate all blocks with object ID of 18 – object ID of the OBJ$ table.
Follow each entry in the row directory
Some of these will point to “live” (0x2C) rows
Others “deleted” (0x3C)
All data that has not been “blocked out” is deleted data – may only be fragments though!
Rinse and Repeat for all “interesting” object IDs – e.g. SOUCRCE$,
<table>
<thead>
<tr>
<th>Ch.</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>00h</td>
<td>12</td>
<td>F4</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>01h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>02h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>03h</td>
<td>0F</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>04h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>05h</td>
<td>01</td>
<td>03</td>
<td>05</td>
<td>01</td>
<td>03</td>
<td>05</td>
<td>01</td>
<td>03</td>
<td>05</td>
<td>01</td>
<td>03</td>
<td>05</td>
<td>01</td>
<td>03</td>
<td>05</td>
<td>01</td>
</tr>
<tr>
<td>06h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>07h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>08h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>09h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0Ah</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0Bh</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0Ch</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0Dh</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0 Eh</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0Fh</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
</tbody>
</table>
F.E.D.S. (Forensic Examiner’s Database Scalpel)

A: Hex Dump
B: Block Info
C: ASCII View
D: Row Data
  Green: “live”
  Red: Deleted
E: Block Number
F: Object ID for block

F.E.D.S. is still in design and research stage
Oracle Redo Logs

Binary file that keeps a record of changes (called redo entries) so in the event of a database failure all actions can be redone.

Redo Entry
Contains all changes for a given SCN (System Commit number)
Header and one or more change vectors
Change Vector operation codes

- 5.1 Undo Record
- 5.4 Commit
- 11.2 INSERT on single row
- 11.3 DELETE
- 11.5 UPDATE single row
- 11.11 INSERT multiple rows
- 11.19 UPDATE multiple rows
- 10.2 INSERT LEAF ROW
- 10.4 DELETE LEAF ROW
- 13.1 Allocate space [e.g. after CREATE TABLE]
- 24.1 DDL

We can use these to determine what actions were taken
INSERT Example
Time stamp

Timestamp is when the redo entry was written – not when the action was taken.

Records to the second from midnight of 1<sup>st</sup> January 1988.
Demo followed by questions

Any questions?
Thank You

http://www.ngsconsulting.com/