Worldwide Trends in Database Threats and Database Security

jacob@sentrigo.com
The basics

No-one is going to say to a DBA:
"Congratulations, no-one stole data from us this year. Here’s a 10% pay raise"

Instead they say:
"Great, we reduced the number of days the database was down for maintenance by 5%"

Source: Anonymous contributor to the "Eye on Oracle" blog
What happened in the last 3 years?

- February 2005: ChoicePoint Breach
  - Credit history information
  - Classic social engineering attack
  - Result: 163k consumer records stolen, $15M in penalties and charges, security audits until 2026...

- December 2005: Guidance Software Inc. Breach
  - 3,800 Credit cards, names and more of professionals from NSA, FBI, CIA...
  - Probably SQL injection attack via the web

- Also in 2005 - -- University of Southern California, Boston College, California State University, Chico and the University of Georgia, Lexis Nexis, PayMaxx, San Jose medical, DSW all suffered high profile data breaches...
This Year

- **July 2005 - January 2007: TJX**
  - 45.7M+ credit/debit card records stolen
  - Sophisticated attack (WiFi -> Internal Network -> DB)
  - Result: data sold to data brokers and used in many scams, TJX faces lawsuits and losses of $25M until May 07 (will grow considerably)

- **July 2007 - Fidelity National Information Services**
  - Bank and credit data of 2.3M customers
  - Stolen by a DBA

- And many more breaches... not only in the U.S. (e.g. Home Office breach in the U.K.)

- Many breaches are unknown or not made public
- Many breaches remain undetected
What else happened during these years?

- Regulations kicking in:
  - SB 1386
  - Sarbanes Oxley
  - PCI-DSS
  - SAS 70
  - and more...

- Bad guys are getting more "professional"
- Perimeter firewalls are doing a better job at protecting databases from external threats
- Outsourcing IT is the norm
- Many databases get closer to the Internet
- Database vendors begin to acknowledge vulnerabilities
Vulnerabilities abound

- The most widely used, diverse and complicated DBMS - Oracle is the center of attention as regards DBMS security threats
- CVE (Common Vulnerabilities and Exposures, an independent security website) lists the no. of vulnerabilities for DBMSs as follows:

<table>
<thead>
<tr>
<th>DBMS</th>
<th>No. of Vulnerabilities</th>
<th>Reported since Jan 2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS SQL</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Sybase</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>DB2</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Informix</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>MySQL</td>
<td>53</td>
<td>53</td>
</tr>
<tr>
<td>Oracle</td>
<td>82</td>
<td>82</td>
</tr>
</tbody>
</table>

No. of vulnerabilities reported since Jan 2006
Oracle database CVEs (Common Vulnerabilities and Exposures)

Total Number of CVEs from 2003 (accumulated)
What are the attack trends we predict?

- **Internet attacks** on databases will have less impact:
  - Better perimeter protection in place
  - Customer awareness to risks higher

- **Insider attacks** on databases have always happened but now have higher exposure:
  - Exposure will lead to more attacks
  - Like network based attacks, benevolent hackers will be replaced by criminals
  - Loyalty of insiders cannot be counted on

- Attacks will become more **sophisticated**:
  - We are still in initial stages of evolution
  - Last Black Hat showed that more sophisticated attacks are possible and vicious
Database security products

- Most are firewalls on steroids:
  - Take the firewall paradigm, apply it to database
  - Based on finding the SQL within network protocol and applying policy to it
  - Yet another appliance to worry about
  - Targeted at security professionals, not DBAs
  - Some add agents to compensate for major blind spots
  - Will end up integrating into perimeter products
- Many homegrown solutions that focus on compliance rather than real security
Another word about compliance

- Important for many reasons
- Often a lot of interpretation is involved
- But it is not security - you can be 100% compliant with any or all regulations but still exposed
- Securing your database, requires a deep understanding of your environment
Hedgehog: Real Database Security

- A host-based software solution that monitors *all* DB transactions in real time
- Prevents improper use by privileged users as well as intruders from the outside
- Preset and administrator-defined rules
- Minimal impact on performance - uses less than 5% of a single CPU
- Full audit trail
Hedgehog Logical Architecture

- SIM/SEM tools
- Alerts
- Hedgehog JavaEE Server (software)
- Hedgehog Console
- Web-based GUI

- Network
- Sensor
- Sensor
- Sensor
- DB
- DB
- DB
Thank You!
How about the bad guys?

<table>
<thead>
<tr>
<th>Year</th>
<th>Date</th>
<th>Exploit Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>25-mar-07</td>
<td>Local Privilege Escalation (win32) - [Become DBA]</td>
</tr>
<tr>
<td>2006</td>
<td>17-nov-06</td>
<td>SQL Injection in KUPW$WORKER - [Become DBA]</td>
</tr>
<tr>
<td>2006</td>
<td>20-apr-06</td>
<td>SQL Injection in dbms_export_extension - [Become DBA]</td>
</tr>
<tr>
<td>2005</td>
<td>27-jan-06</td>
<td>Buffer overflow DBMS_XMLSCHEMA - [Crash File on Database Server]</td>
</tr>
<tr>
<td>2005</td>
<td>27-jan-06</td>
<td>Buffer overflow DBMS_XMLSCHEMA_INT - [Create Remote Shell]</td>
</tr>
<tr>
<td>2005</td>
<td>01-may-05</td>
<td>OS command injection in DBMS_SCHEDULER - [Become DBA]</td>
</tr>
<tr>
<td>2005</td>
<td>13-apr-05</td>
<td>SQL Injection vulnerability in DBMS_METADATA - [Become DBA]</td>
</tr>
<tr>
<td>2005</td>
<td>13-apr-05</td>
<td>SQL Injection vulnerability in DBMS_CDC_SUBSCRIBE / DBMS_CDC_SUBSCRIBE - [Become DBA]</td>
</tr>
<tr>
<td>2005</td>
<td>15-apr-05</td>
<td>Denial of service vulnerability in Oracle Intermedia [Denial of Service]</td>
</tr>
<tr>
<td>2005</td>
<td>2-may-05</td>
<td>Become DBA via DBMS_SYS_SQL (Become DBA)</td>
</tr>
<tr>
<td>2005</td>
<td>2-may-05</td>
<td>Switch username to SYS after executing a job via DBMS_SCHEDULER [Switch Username]</td>
</tr>
</tbody>
</table>

- Exploits for Oracle 10g only
- Only exploits that are already patched presented here, and this is a good site...
- Source: red database security