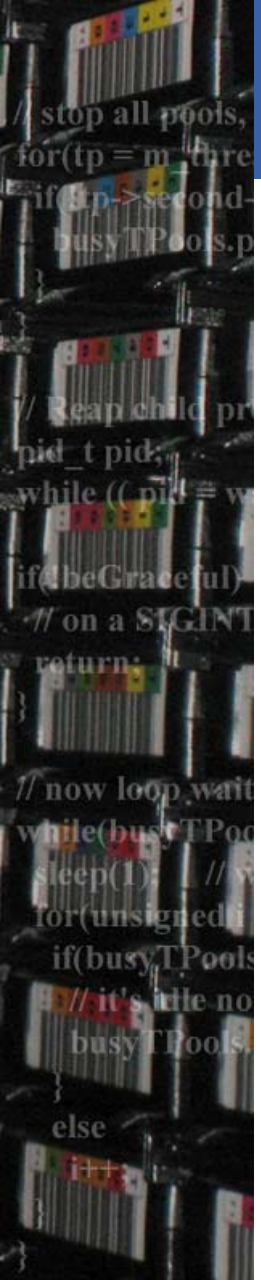

Security Overview

Luca Canali, CERN

Distributed Database Operations Workshop

April 20-21 2009, Barcelona

Outline

- Review of database security
  - Sharing experiences
  - Coordinate homogeneous effort across 3D community
- Main areas of interest
  - Threats to DB-centric applications
  - Actions to mitigate risks
  - Procedures and policies

DB Security Threats

- Databases and DB applications are vulnerable at various levels, notably:
  - DB-specific security bugs
  - Application-related vulnerabilities
  - User-related vulnerabilities
  - External vulnerabilities (network, OS, etc)
- Risks:
  - Unauthorized access, defacing, worms, downtime, serious damage
  - Negative press exposure
  - Data theft

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

DB Security Bugs 1/3

- DB-specific bugs are addressed by Oracle's CPU patches
  - Many fixes are for internal packages who suffer SQL injection or other major vulnerabilities
  - CPU patches expose the vulnerabilities to the community -> exploit come out on the internet
  - CPU patches come with a score for the vulnerability
  - The most dreaded are vulnerabilities that can be remotely exploited
  - Incidents like SQL slammer worm may happen again

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

DB Security Bugs 2/3

- Our experience
  - Apply CPU patches asap (after a validation period of about 3 weeks)
  - Users' privileges are limited to the necessary set (no 'any' operations to users)
  - Read only accounts are treated as the read-write accounts for access security (privilege escalation is a big risk)
  - Read regularly blogs and security mailing lists for new threats, exploits, etc
  - Coordination within IT with the security team and between DBAs

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

DB Security Bugs 3/3

- Our experience
  - Many packages in Oracle are ‘grated to public’, we revoke at installation some that are know to have (or have had) security flaws

```
revoke execute on sys.lt from public;
revoke execute on dbms_cdc_subscribe from public;
revoke execute on dbms_cdc_isubscribe from public;
revoke execute on sys.utl_tcp from public;
revoke execute on sys.utl_http from public;
revoke execute on sys.utl_smtp from public;
revoke execute on sys.dbms_export_extension from
   public;
```

Application Related Vulnerabilities 1/2

- Applications' vulnerabilities open the way to DB access
  - SQL injection is a typical example
  - Other vulnerabilities of the app server can give an attacker full control on DB connection
  - A simple mistake on the application code can open the way for attacker to execute arbitrary SQL at least on one schema

Application Related Vulnerabilities 2/2

- Our experience
  - During validation phase we look at possible vulnerabilities
  - Recent example: suggested use of bind variables against SQL injection
  - Other example: protect the application with NICE credentials (see DB monitoring)
  - For our own ‘DBA applications’: we take care not to expose passwords
  - Overall it’s the developers’ responsibility to secure the application but DBAs can provide useful feedback

Users' Generated Vulnerabilities 1/2

- Users can fail to protect the DB access
  - They may open easy way for an attacker to enter the DB
  - Social engineering is also a threat
  - Overall a collaborative environment is more prone to security holes

Users' Generated Vulnerabilities 2/2

- Our experience
  - We use a password scanner to warn users of weak passwords + we force password complexity (and account expiration)
  - We keep track of account owners
  - Accounts and passwords can leak on the internet and search engines
  - Tnsnames can also leak to google
  - CVS is another potential pitfall
  - Wikis and monitoring tool should take care not to expose too much information on the setup
  - Overall it's the users' responsibility, DBAs can put in place tools and awareness of risks to help

External Vulnerabilities

- The OS and network need to be protected too:
  - Other (non-Oracle) vulnerabilities can be used to enter the DB
  - If an attacker can break into the server, the DB is owned too

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

External Vulnerabilities

- Our experience
  - Firewall access to DB server
  - Add local iptable firewall
  - Use non-default listener port
  - Regularly apply OS patches as provided by Linux support
  - Patches are applied in a rolling way, on scheduled maintenance

Challenges of a distributed environment

CERN IT Department

- In a distributed environment if one target is broken into, the others may be at risk

- Our experience
  - None so far, fortunately!
  - CERT IT security team and service managers will work together in case of security issues

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Digression on CPU Patches

- Are CPU patches adding security to the system?
  - It is found that several Oracle users do not apply CPU patches at all
  - They rely on securing the DB with firewalls and/or hoping for the best!
  - Old method of ‘securing’ the DB, where one would also find weak password

Digression on CPU Patches

- The answer in my opinion is yes, but only if the CPU patches are applied in a timely manner
  - After CPUs are out, details on the vulnerability come out too from security experts
  - It makes easy for non-experts to build exploits
  - One can also simply look at the patch files and find vulnerable pieces of code
  - Example CPU Apr09 has a sql injection vulnerability in a procedure inside dbms_aqadm_sys that can be easily seen just comparing old and new code!
  - Another example, CPU APR09 exposes that Oracle 9.2.0.8 has a high score vulnerability on the resource manager

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Auditing

- Auditing
  - In auditing logs there is a large amount of information that can be used for security purposes
  - Identify unauthorized logons or attempts
  - OS and DB auditing can be used together
  - DB auditing can produce a lot of information and have a high performance impact
  - Our experience: to use auditing it's necessary to have a 'clean up job' too or the audit table will fill up quickly.
  - Custom scripts and EM functionality have already some processing of audit logs at CERN

AUDITMON project

- AUDITMON
  - A project that has been recently started, collaboration IT-DM, IT-DES
  - A tool to automate the analysis of logon auditing
  - Will be customized for each experiment
  - Will make use of a common repository of audit data
  - Will work with rules (2 sets: one to move audit data to the repository and one to process data)

Other Areas of Oracle Security

- Security policies and actions can grow to be highly sophisticated, depending on the industry. It's worth mentioning:
  - Encryption of Oracle*net traffic
  - Encryption of Oracle data and/or backups
  - DDL auditing
  - DML auditing
  - DB privilege usage auditing
  - Fine grained data access
  - Auditing of DBA actions
  - Penetration testing

Summary

- DB security status is no different from other applications areas
- Multiple threats and security risks are identified
- Keeping the infrastructure secure is an ongoing process (and a ‘moving target’ too)
- In a distributed environment sharing experiences is a must