Oracle Database Security Case Study

演讲人：罗海雄

职务：云和恩墨，性能优化及安全总监

日期：2014,09,24

微博： @SeroLL

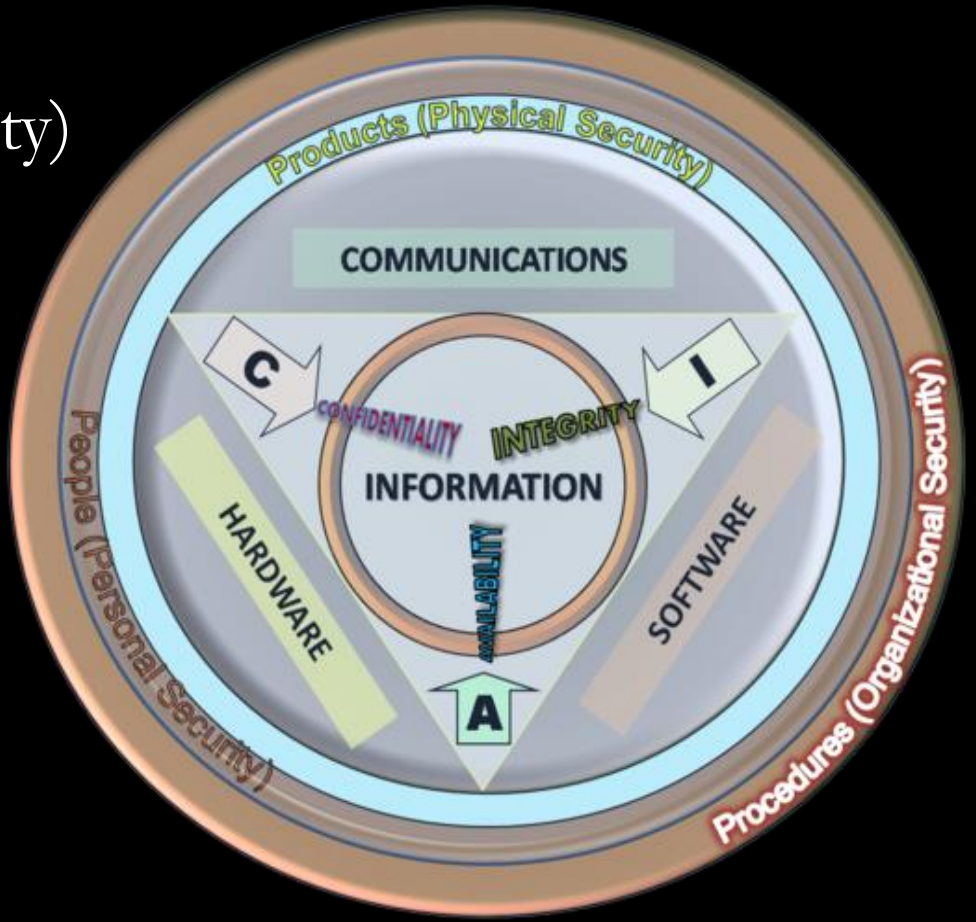
邮件： haixiong.luo@enmotech.com

今日热词：脱裤？

- 数据库是精华所在
- 相对于单个账号被盗，整库被盗是最致命的

信息安全：三个要素

- 信息安全三要素(CIA)
  - 保密性(Confidentiality)
  - 完整性(Integrity)
  - 可用性(Availability)



信息安全：十个Domain

1、访问控制

2、远程通信安全

3、风险管理及连续性计划

4、规章与制度

5、架构及系统安全

6、法律、法规、合规性和调查

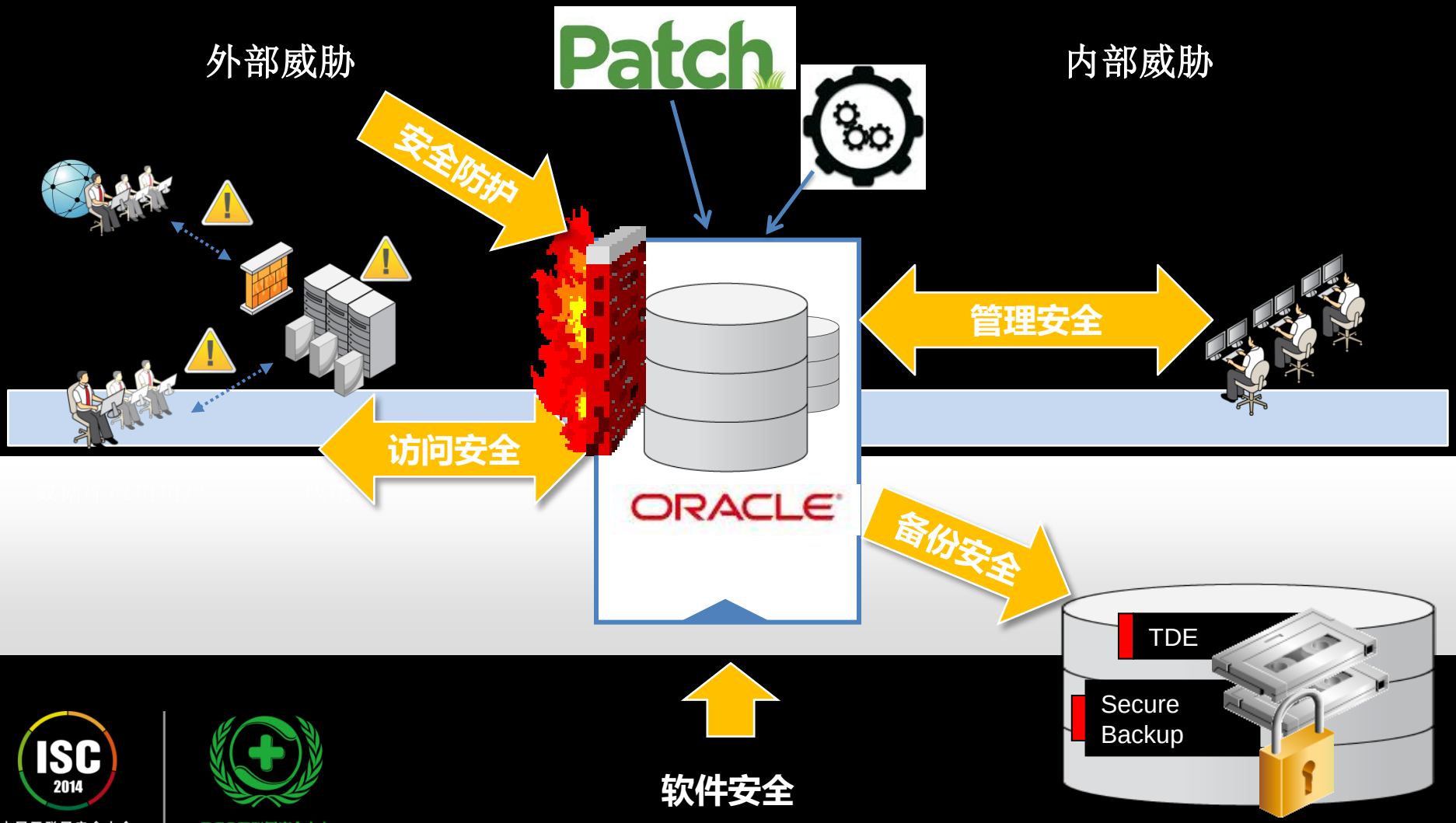
7、应用程序安全

8、密码学

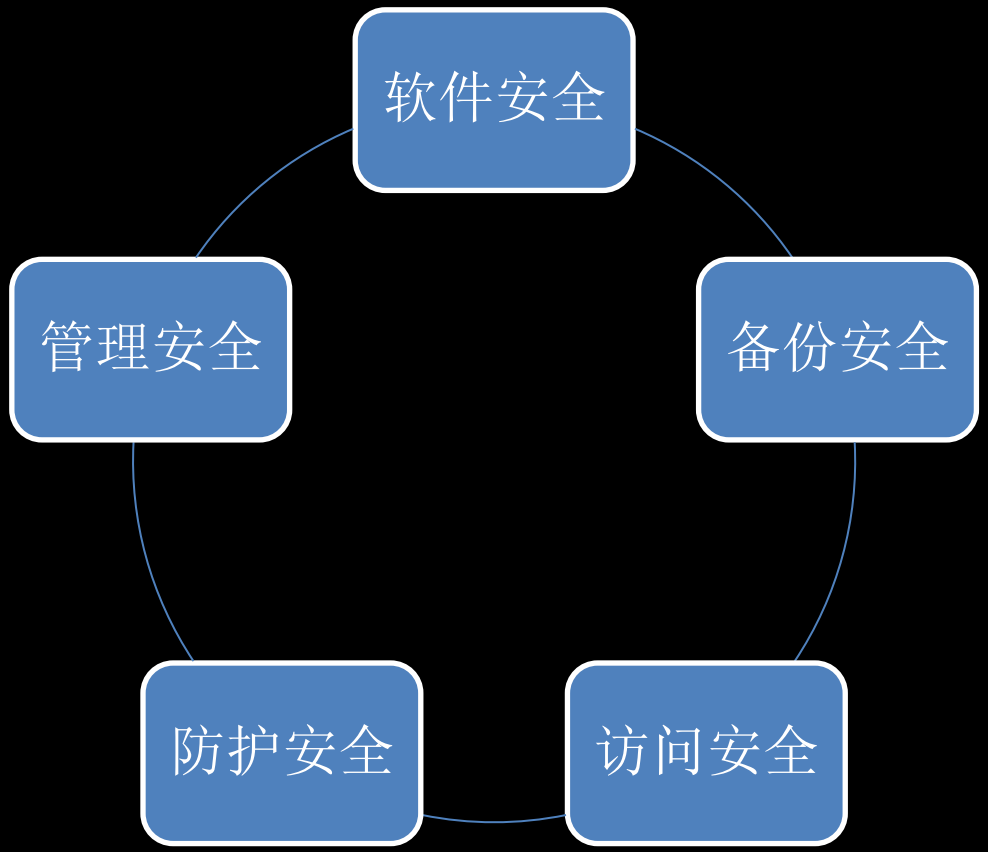
9、操作安全

10、物理安全

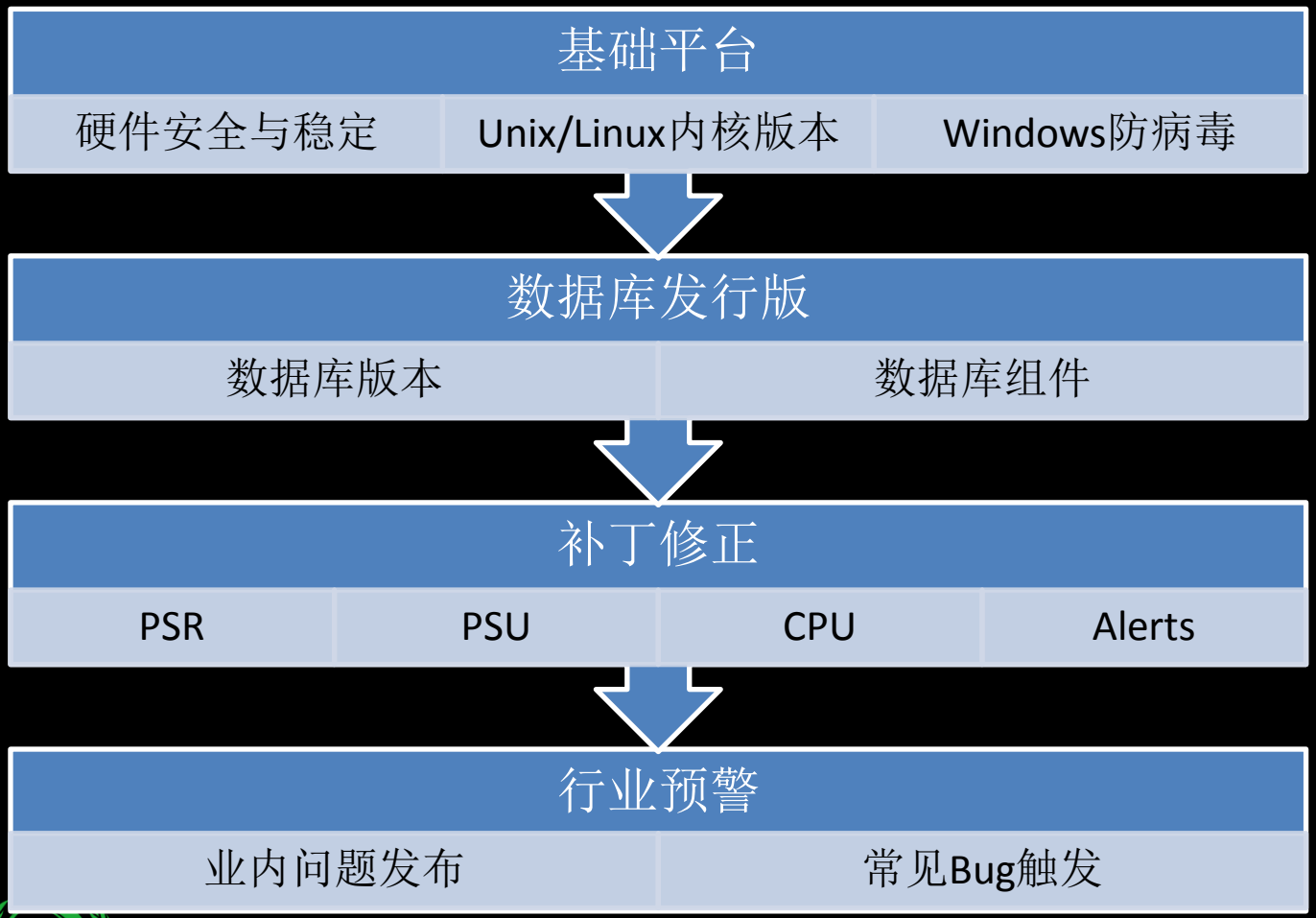
数据库安全-威胁来自何方？



数据库安全-安全的五大方向



数据库安全-软件安全


基础平台
硬件安全与稳定
Unix/Linux内核版本
Windows防病毒
数据库发行版
数据库版本
数据库组件
补丁修正
PSR
PSU
CPU
Alerts
行业预警
业内问题发布
常见Bug触发

软件安全-安全补丁和组件安全

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-5853				2014-01-15	2014-03-05	5.0	None	Remote	Low	Not required	None	None	Partial
Unspecified vulnerability in the Core RDBMS component in Oracle Database Server 11.1.0.7, 11.2.0.3, and 12.1.0.1 allows remote attackers to affect availability via unknown vectors.														
2	CVE-2013-3826				2013-10-16	2013-11-02	5.0	None	Remote	Low	Not required	Partial	None	None
Unspecified vulnerability in the Core RDBMS component in Oracle Database Server 11.1.0.7, 11.2.0.2, 11.2.0.3, and 12.1.0.1 allows remote attackers to affect confidentiality via unknown vectors.														
3	CVE-2013-1554				2013-04-17	2013-10-10	5.0	None	Remote	Low	Not required	None	None	Partial
Unspecified vulnerability in the Network Layer component in Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, and 11.2.0.3 allows remote attackers to affect availability via unknown vectors.														
4	CVE-2013-1538				2013-04-17	2013-10-10	5.0	None	Remote	Low	Not required	None	None	Partial
Unspecified vulnerability in the Network Layer component in Oracle Database Server 11.2.0.2 and 11.2.0.3 allows remote attackers to affect availability via unknown vectors.														

软件安全-安全补丁和组件安全

-

```
SQL> connect scott
Enter password:
Connected.
SQL> @run.sql

Package created.


Package body created.


PL/SQL procedure successfully completed.

SQL> select * from user_role_privs;

USERNAME                       GRANTED_ROLE                   ADM DEF OS_
------------------------------ ------------------------------ --- --- ---
SCOTT                          CONNECT                        NO  YES NO
SCOTT                          DBA                            NO  YES NO
SCOTT                          RESOURCE                       NO  YES NO
```

软件安全-行业案例及软件BUG

-
-

Bug 8198906 OERI [kddummy_blkchk] / OERI [5467] for an aborted transaction of allocating extent

This note gives a brief overview of bug 8198906.
The content was last updated on: 19-JAN-2011
Click here for details of each of the sections below.
This bug is alerted in Note:1229669.1

Affects:

Product (*Component*)	Oracle Server (Rdbms)
Range of versions *believed* to be affected	Versions >= 9.2 but BELOW 11.2
Versions *confirmed* as being affected	• 10.2.0.4 • 10.2.0.3 • 9.2.0.8 • 9.2.0.6
Platforms affected	Generic (all / most platforms affected)

Note that this fix can cause / expose the problem described in Bug:9711859

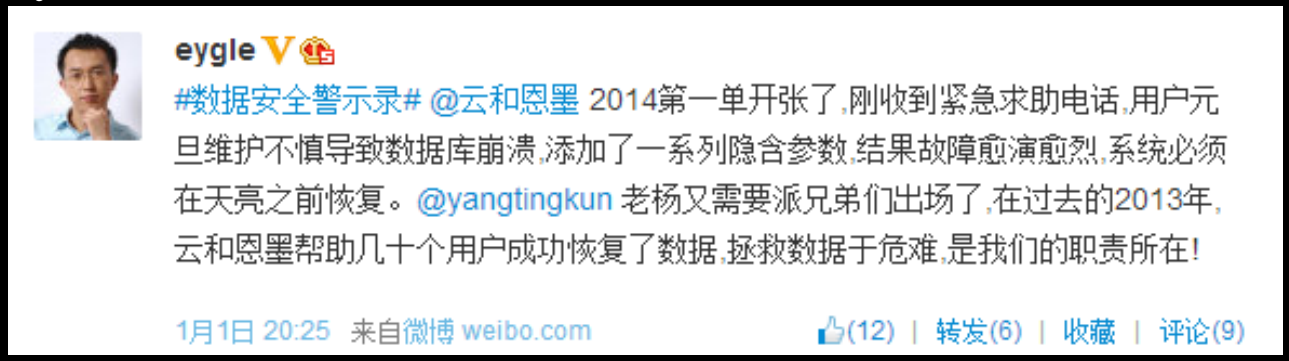
Note that this fix has been superceded **by the fix in** Bug:9711859

Fixed:

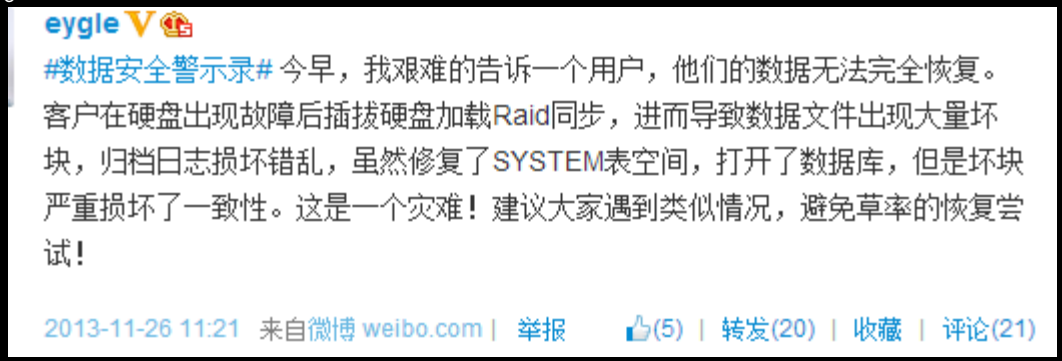
This issue is fixed in	• 11.2.0.1 (Base Release) • 10.2.0.5 (Server Patch Set) • 10.2.0.4 Patch 22 on Windows Platforms

备份安全-备份重于一切

每年都有很多客户主动找上门，需要对生产系统进行紧急恢复。



多数运气好，可以通过底层文件进行恢复。运气不好的，恢复就不完整了。



备份安全-备份重于一切

2014年4月，某知名银行数据库所用存储崩溃，缺乏最新的可用备份.....

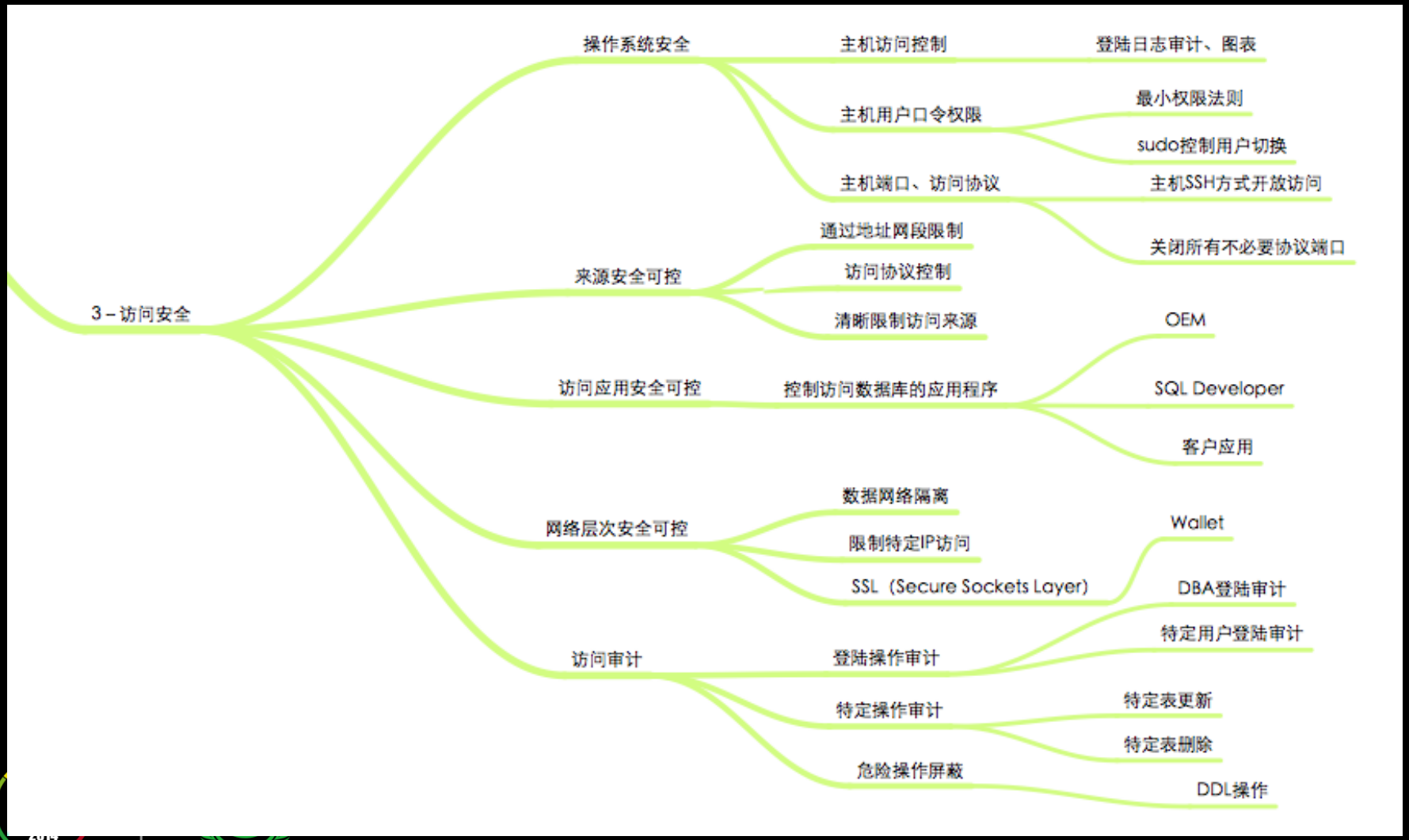
2014年7月，武汉光谷某企业数据库崩溃，还是缺乏可用备份.....

备份，也许是最后的救命稻草！！

备份安全-备份集自己安全吗？

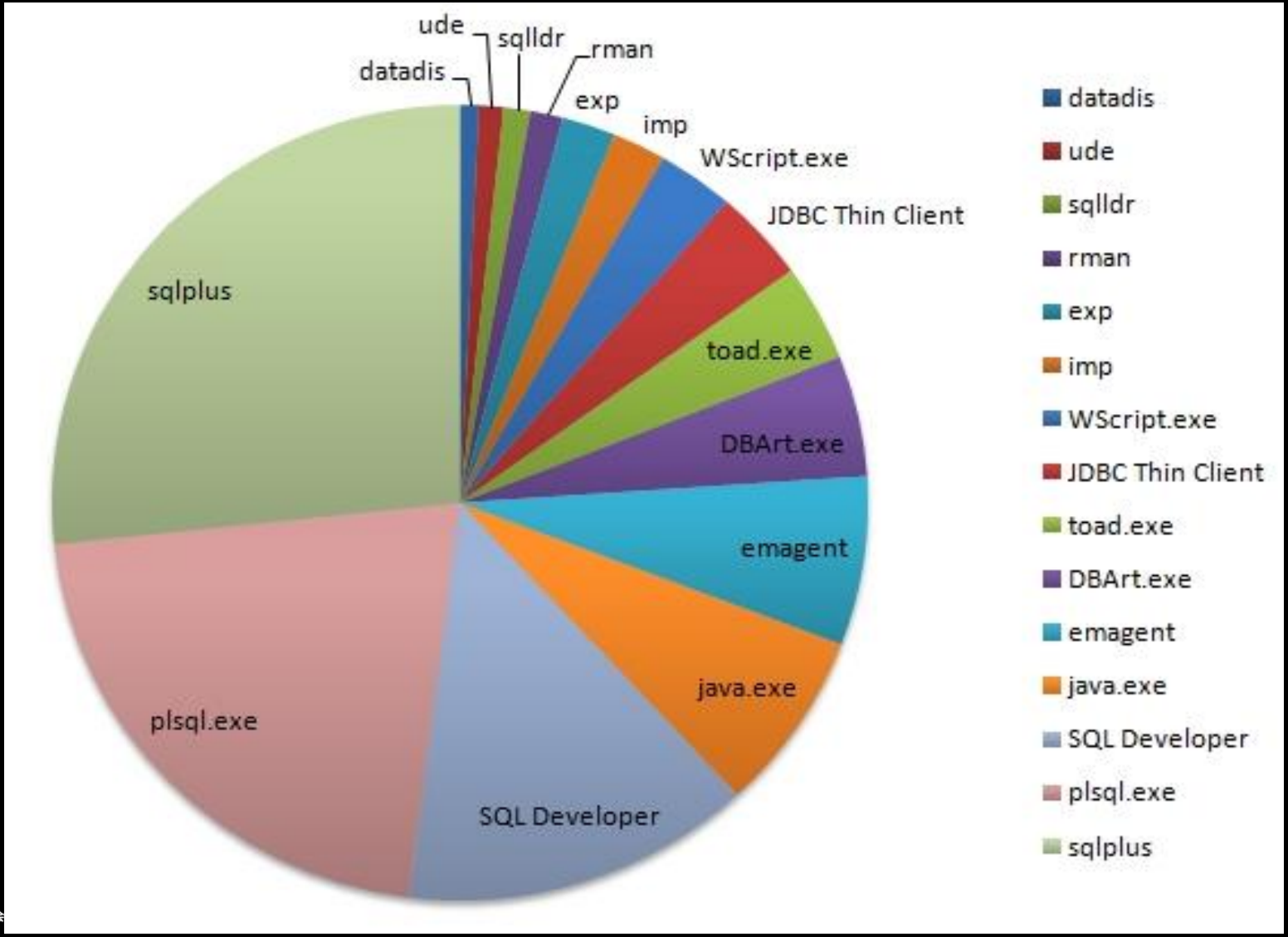
生产库保护足够严密！！
可备份库/备份集存放的机器呢？
万一被盗.....

访问安全-4W1H


3－访问安全
操作系统安全
主机访问控制
登陆日志审计、图表
主机用户口令权限
最小权限法则
sudo控制用户切换
主机端口、访问协议
主机SSH方式开放访问
关闭所有不必要协议端口
来源安全可控
通过地址网段限制
访问协议控制
清晰限制访问来源
访问应用安全可控
控制访问数据库的应用程序
OEM
SQL Developer
客户应用
网络层次安全可控
数据网络隔离
限制特定IP访问
SSL（Secure Sockets Layer)
Wallet
访问审计
登陆操作审计
DBA登陆审计
特定用户登陆审计
特定操作审计
特定表更新
特定表删除
危险操作屏蔽
DDL操作

访问安全-明确访问来源

访问安全-明确访问来源


ude
sqlldr
rman
datadis
exp
imp
WScript.exe
JDBC Thin Client
sqlplus
toad.exe
DBArt.exe
emagent
java.exe
plsql.exe
SQL Developer
datadis
ude
sqlldr
rman
exp
imp
WScript.exe
JDBC Thin Client
toad.exe
DBArt.exe
emagent
java.exe
SQL Developer
plsql.exe
sqlplus

全-SQL注入攻击

心设计的SQL, 让原本正常的SQL执


```
v_userid=request.getParameter("userid");
v_password = request.getParameter("password");
v_password_encrypt= PasswordTools.encrypt("password");
SQL = "select userid,username ...
From t_user_credential
```


```
select userid,username ...
From t_user_credential
Where userid = 'admin' or (1=1 and rownum=1) -- and
password_encrypt  = ...
```

--是注释符

访问安全-SQL注入攻击

摈弃SQL拼接，使用绑定变量，轻松防御SQL注入攻击

```
v_userid=request.getParameter("userid");
v_password = request.getParameter("password");
v_password_encrypt= PasswordTools.encrypt("password");
SQL = "select userid,username ...
From t_user_credential
Where userid = :userid and password_encrypt
=:password_enc" ;
pstmt= prepareStatement(SQL);
pstmt.set(1, v_userid);
pstmt.set(2, v_password_encrypt);
pstmt.execute(...)
```

防护安全-从零开始

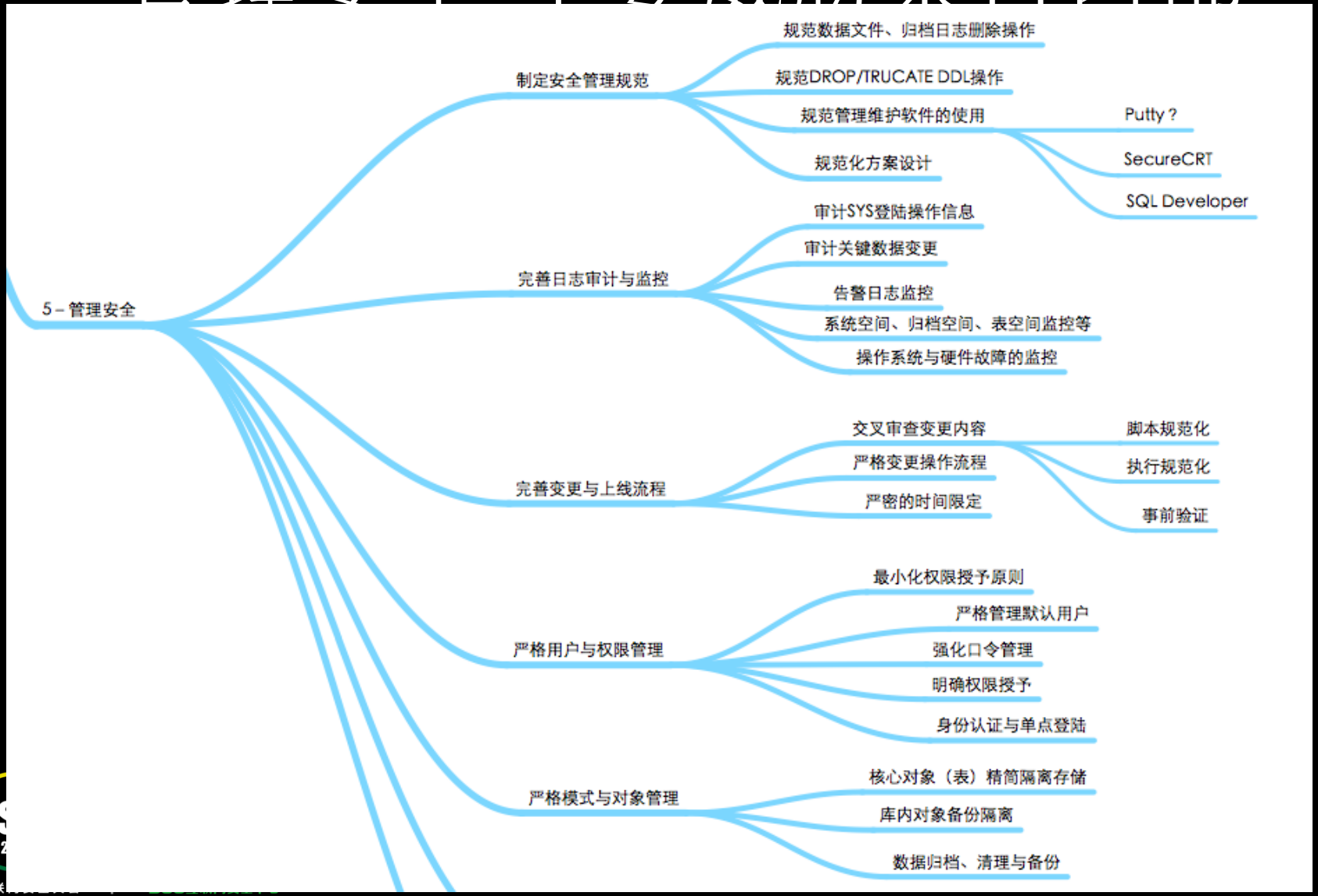
口令的加密内容存储在底层的核心表（USERS是 Oracle 数据库的元数据表之一）中，以下 PASSWORD 字段存储的是 DES 加密值，SPARE4 存储的是 SHA-1 加密串：

```
SQL> select * from v$version where rownum <2;

BANNER
--------------------------------------------------------------------------------
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production

SQL> select name,password,spare4 from user$
  2  where name in ('SYS','SYSTEM','EYGLE');

NAME       PASSWORD         SPARE4
---------- ---------------- ----------------------------------------------------
SYS        8A8F025737A9097A S:BBEFC8B86319E6A40372B9584DBCCA6B015BFE0C7DDF5B9593FB618E0D80
SYSTEM     2D594E86F93B17A1 S:C576FB5A54D009440AC047827392215C673528067BC06659EC56E3178BAB
EYGLE      B726E09FE21F8E83 S:65857F36842AEE4470828E9BE630FEED90A67CEF0D2B40C9FE9B558F6B49
```

重视安全问题，是安全增强的第一要义！

触发器

管理安全-主要威胁来自内部



防护安全-提升请从今日始

Oracle Database 12c

SQL Redaction

Data Masking

Oracle Database 11g

TDE Tablespace Encryption

Oracle Total Recall

Oracle Audit Vault

Oracle Database Vault

Oracle Database 10g

Transparent Data Encryption (TDE)

Real Time Masking

Oracle Database 9i

Secure Config Scanning

Fine Grained Auditing

Oracle Label Security

Enterprise User Security

Oracle8i

Virtual Private Database (VPD)

Database Encryption API

Strong Authentication

Oracle7

Native Network Encryption

Database Auditing

Government customer

ISC 2014 中国互联网安全大会

360互联网安全中心

管理安全-加强规范 提升安全

- 数据篡改案例
  - 某电信客[illegible]息，最后查明[illegible]将进行篡改[illegible]
- 数据窃[illegible]
  - 新闻曾经报[illegible]手机用户信息遭窃取”，案件导致陕西省近1400万手机用户的个人信息被泄露。泄露是由于软件开发人员植入了恶意代码。

日防夜防，家贼难防

管理安全-防家贼

- 防DBA/SA/备份管理员
  - 权责分离 – Oracle Database Vault
  - 文件加密：数据文件透明加密，备份集加密
  - 操作审计：Audit Vault/数据库防火墙
- 防应用管理员
  - 数据库防火墙
  - 操作审计：Audit Vault

Thanks!

罗海雄，云和恩墨，性能优化及安全总监
微博： @SeroLL
邮件： haixiong.luo@enmotech.com