数据安全

第2章 数据安全生态圈

计算机与大数据学院 刘延华

福州大学
FUZHOU UNIVERSITY

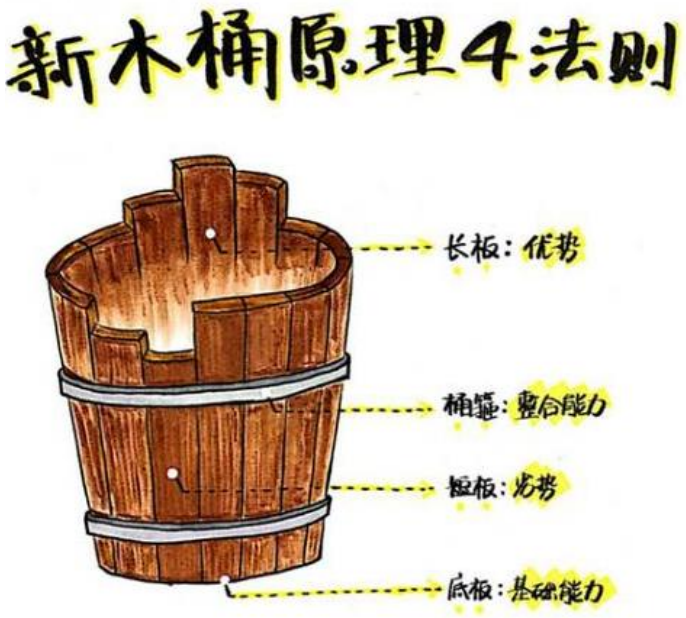
第2章 数据安全生态圈

2.1 数据安全生态圈

口 它是一个安全防护架构的生态圈

从安全防护层次或架构上，进入数据安全3.0时代，全方位安全能力，包括：物理安全、系统安全、网络安全、应用安全，为数据安全提供基础性安全能力保证.

安全能力符合**木桶原则**，防护体系要完整、有力.



2.1 数据安全生态圈

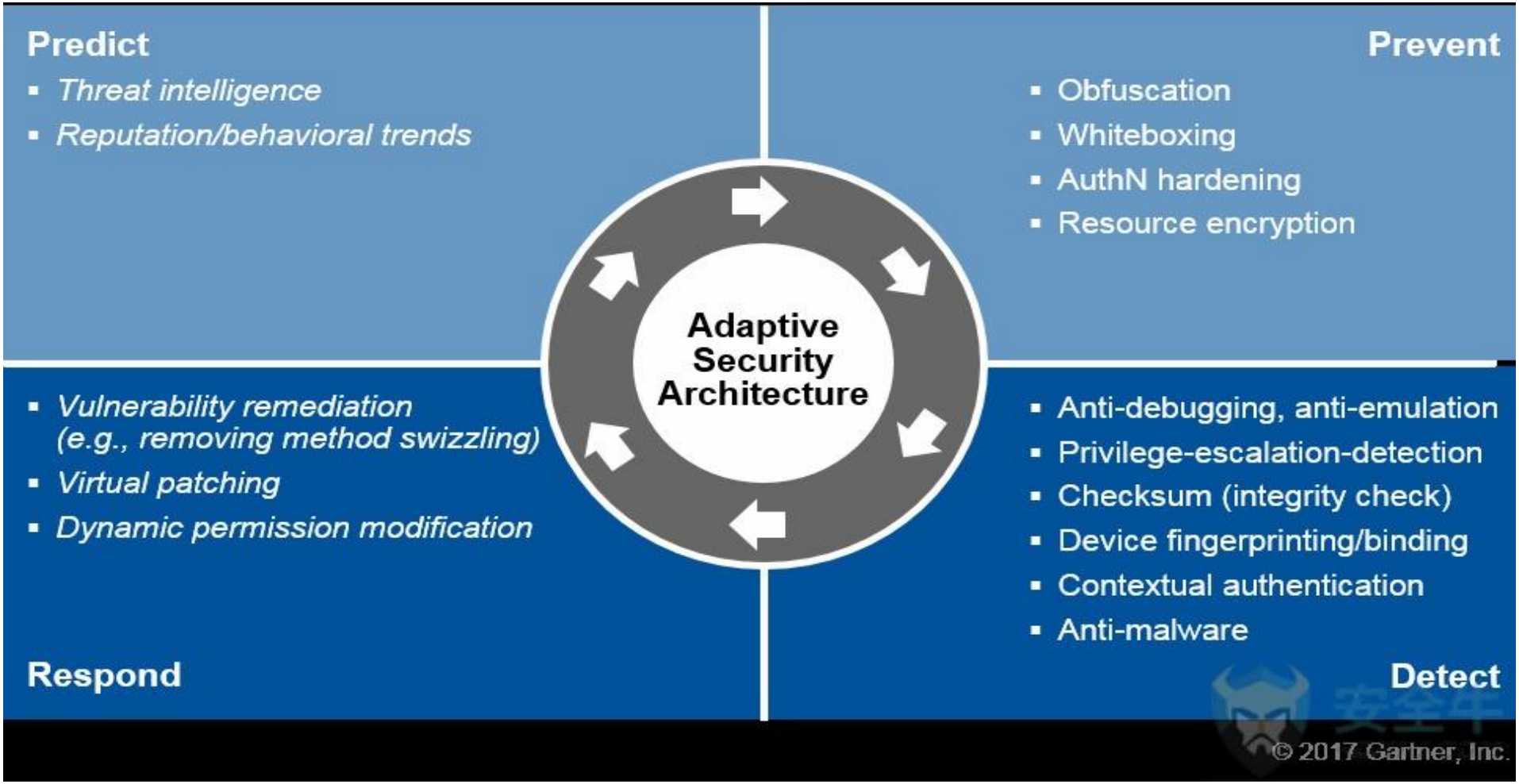
口 它是一个安全模型架构的生态圈

P2DR模型示意图

1999 美国ISS公司提出

- 一个基本的闭环；
- 防护，而非防御；
- 被动因素较多；

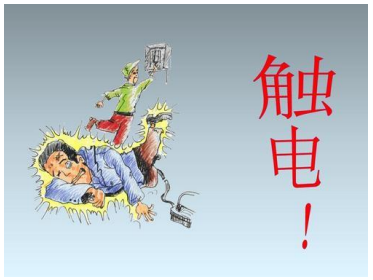
2.1 数据安全生态圈



Gartner 2017：在不同阶段引入威胁情报、大数据分析等新技术和服务，旨在构建一个能进行持续性威胁响应、智能化、协同化的安全防护体系。

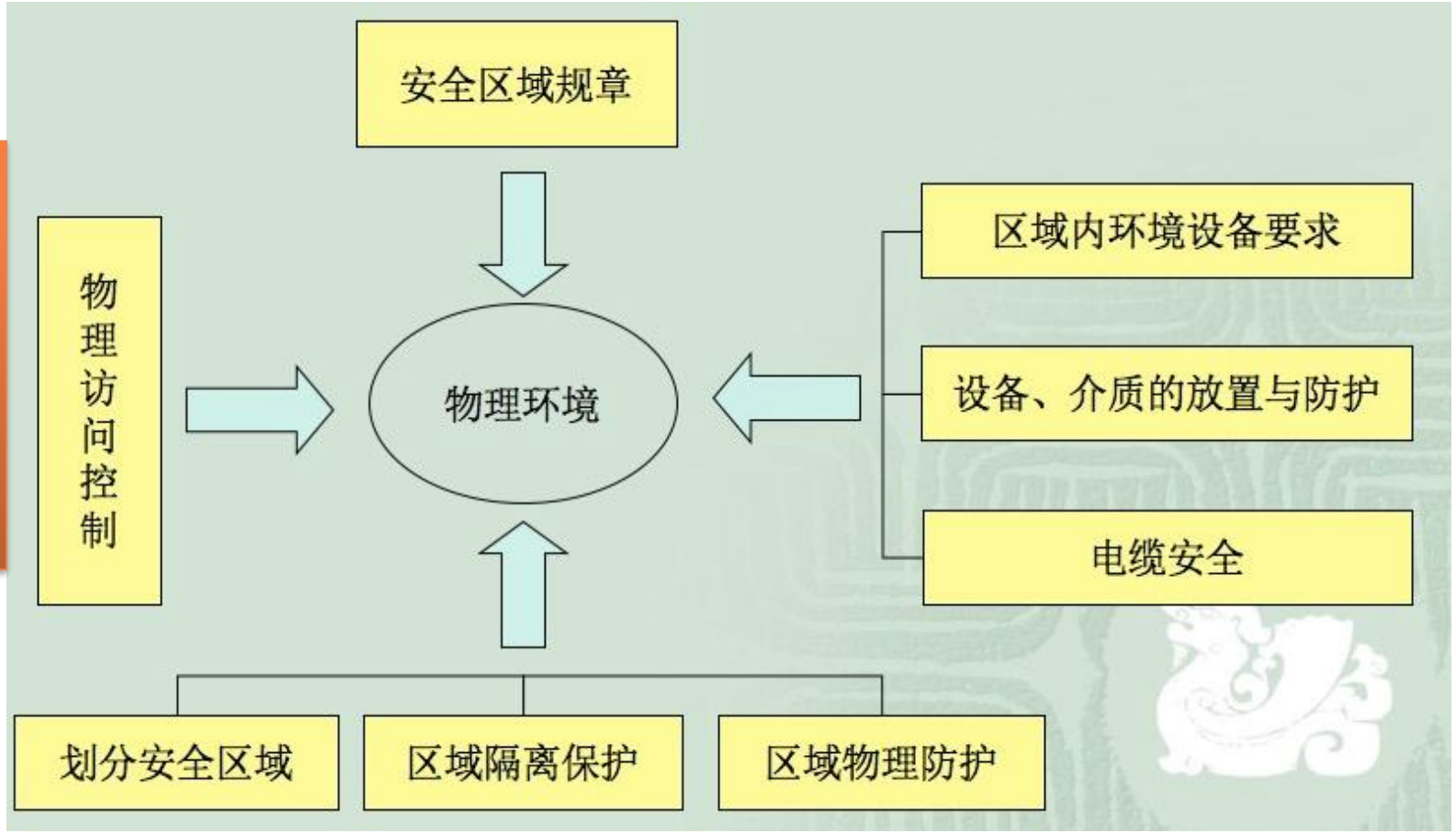
2.2 物理安全

- **定义：**为了保证信息系统安全可靠运行，确保信息系统在对信息进行采集、处理、传输、存储过程中，不致受到人为或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施（包括机房建筑、供电、空调）、环境人员、系统等采取适当的安全措施。（**2007年版**）
- 物理安全是最基础的，同时也是最重要的，是整体信息安全的基础，如果管控不善会导致致命的损失.



2.2 物理安全

环境安全
设备安全
通信安全
人员安全



数据安全

2.3 操作系统安全

■ 没有操作系统的安全性，就没有主机系统的安全性，从而也没有网络系统的安全性。可以说，操作系统安全是信息安全的基石。

✓ 操作系统中已发现且已公开**安全漏洞**已超过10000个，且近年来呈倍数级增长态势。（2016年，之后每年近1000个新增）

✓ 高等级的安全操作系统研发一直是国家级安全战略！

✓ 银河麒麟操作系统

2.3 操作系统安全

安全操作系统：安全操作系统是按照特定安全目标设计实现的操作系统，和符合标准的安全等级相对应。

依据特定的安全等级标准，采用满足条件的安全策略、安全模型和安全机制设计实现，消除安全威胁和安全漏洞可能带来的风险，保证操作系统安全运行的操作系统。

2.3 操作系统安全

- **关键技术：**

✓ 用户标识与鉴别：安全登录

✓ 访问权限控制：自主、强制

✓ **最小特权管理机制**：超级用户

✓ 安全审计：可审计性

✓ 口令安全性：口令长度、强度限制

✓ **安全内核**：保护OS本身安全

✓ **客体重用**：非授权共享内存问题

2.4 网络安全

□ 术语：网络安全

定义：是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

--《中华人民共和国网络安全法》

2.4 网络安全

- 网络不安全的原因
  - ✓ 网络自身缺陷
  - ✓ 网络的开放性
  - ✓ 黑客攻击的攻击

自身缺陷

- 服务器应用系统存在很多漏洞
- 密码保密措施不强，管理乱
- 数据加密强度不高，易破解
- 网络协议并不安全
- 网络操作系统安全级别较低
- 各种应用程序存在着安全问题

网络开放性

- 业务基于公开的协议
- 远程访问使得各种攻击无需到现场就能得手
- 连接是基于主机上的区域彼此信任的原则

黑客（HACKER)的攻击

定义：“非法入侵者”
起源：60年代
目的：基于兴趣非法入侵
基于利益非法入侵
信息战

2.5 数据(库)系统安全

- 数据(库)安全包含两层含义：

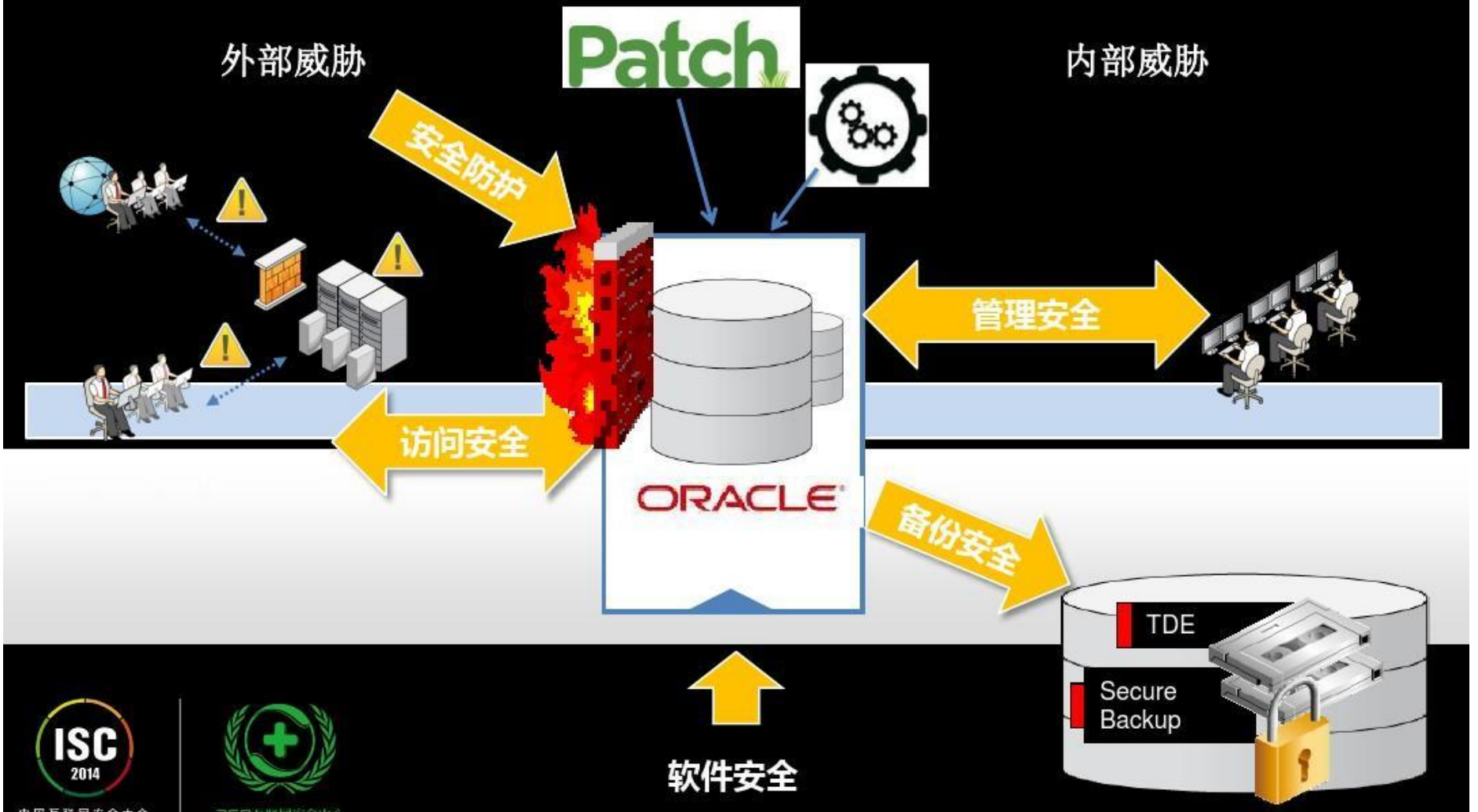
第一层 是指**数据(库)系统运行安全**，包括其所在的宿主系统运行安全。

第二层 是指**数据信息安全**，即所存储数据的安全。我们通常所说的数据库安全，更倾向于指数据的安全。

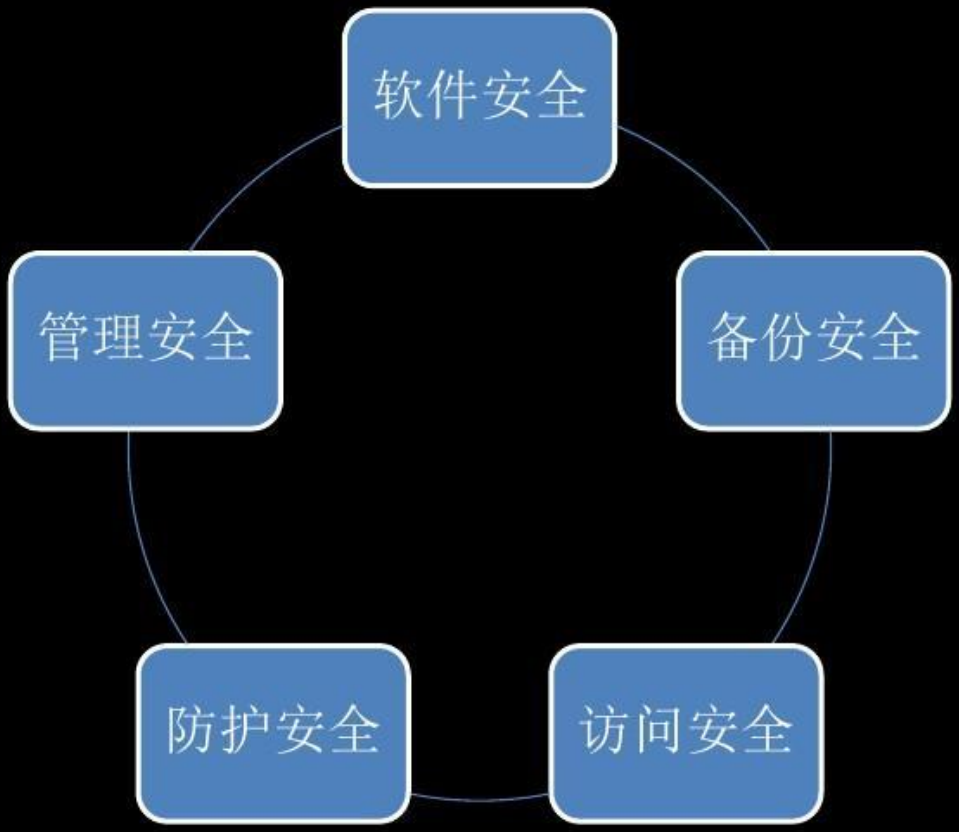
数据库防火墙

福州大学
FUZHOU UNIVERSITY

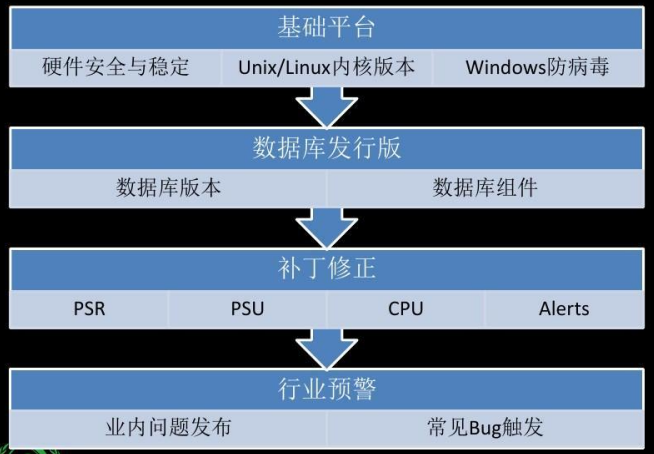
数据库安全-威胁来自何方？



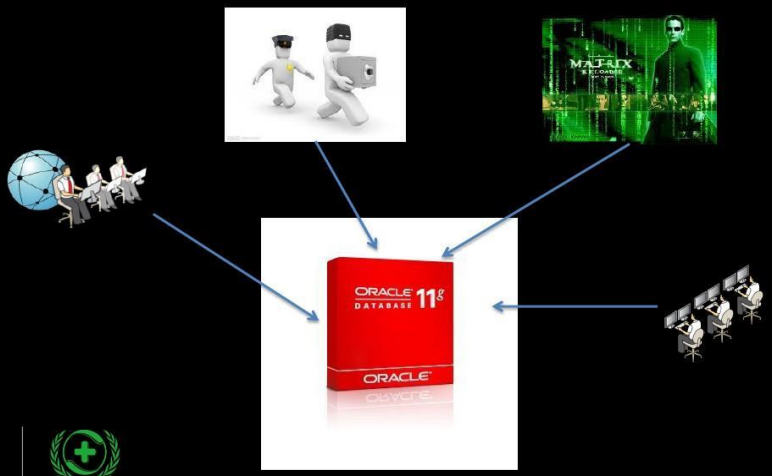
数据库安全-安全的五大方向



数据库安全-软件安全



访问安全-明确访问来源



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.....

备份集加密
！！

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:BBEFCBB86319E6A40372B9584DBCCA6B015BFE0C7DDF5B9593FB618E0D80
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

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 10g
- Oracle Database Vault
- Transparent Data Encryption (TDE)
- Real Time Masking

Oracle Database 9i
- Secure Config Scanning
- Fine Grained Auditing
- Oracle Label Security
- Enterprise User Security
- Virtual Private Database (VPD)

Oracle8i
- Database Encryption API
- Strong Authentication
- Native Network Encryption

Oracle7
- Database Auditing
- Government customer

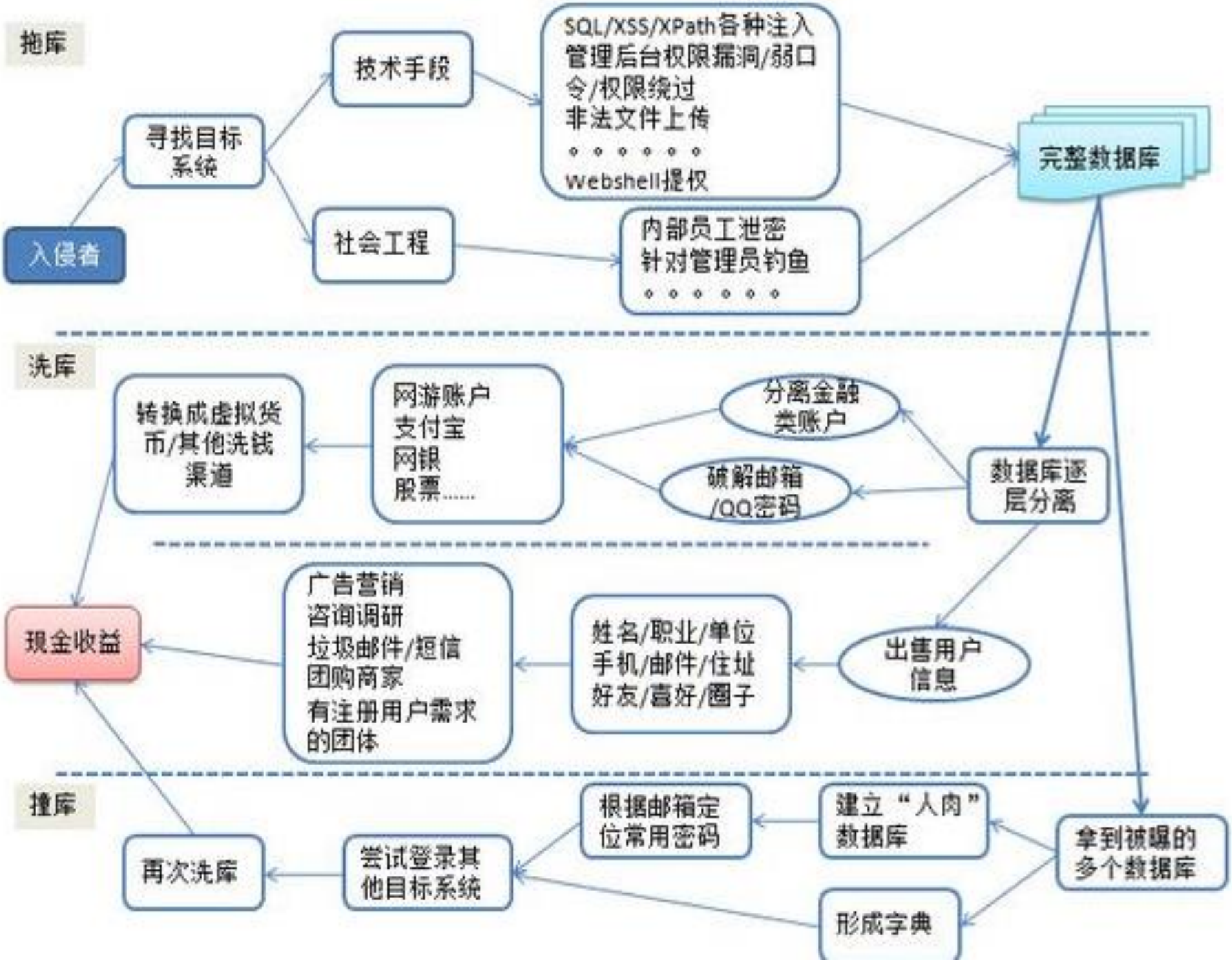
管理安全-加强规范 提升安全

- 数据篡改案例
  - 某电信客[illegible]息，最后查明[illegible]器进行篡改[illegible]
- 数据窃[illegible]
  - 新闻曾经报[illegible]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


拖库
技术手段
SQL/XSS/XPath各种注入
管理后台权限漏洞/弱口令/权限绕过
非法文件上传
。。。。。。
Webshell提权
寻找目标系统
入侵者
社会工程
内部员工泄密
针对管理员钓鱼
。。。。。。
完整数据库
洗库
转换成虚拟货币/其他洗钱渠道
网游账户
支付宝
网银
股票.....
分离金融类账户
破解邮箱/QQ密码
数据库逐层分离
现金收益
广告营销
咨询调研
垃圾邮件/短信
团购商家
有注册用户需求的团体
姓名/职业/单位
手机/邮件/住址
好友/喜好/圈子
出售用户信息
撞库
再次洗库
尝试登录其他目标系统
根据邮箱定位常用密码
建立“人肉”数据库
拿到被曝的多个数据库
形成字典

2.6 应用系统安全

- 服务器软件安全性
- 客户端软件安全性
- APP应用安全性
- 应用软件层出不穷，恶意的和非恶意的安全问题都很严重

Web防火墙

邮件网关

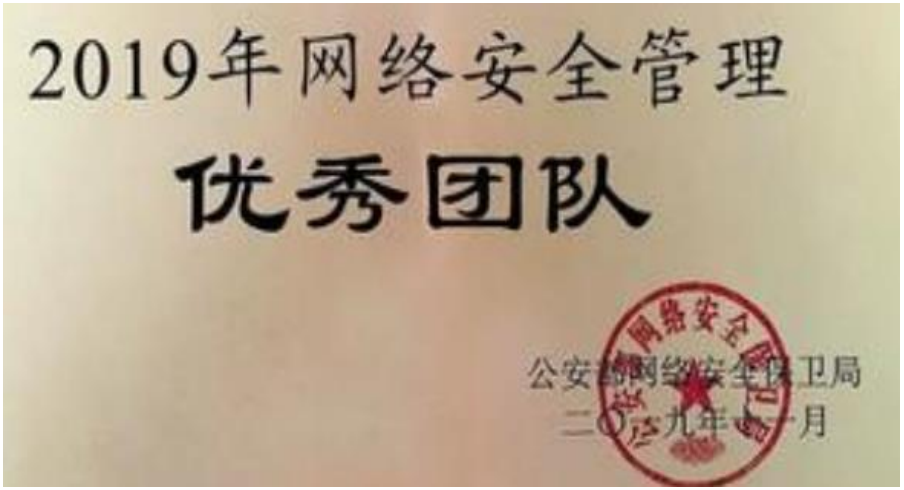
恶意代码检测

应用网关

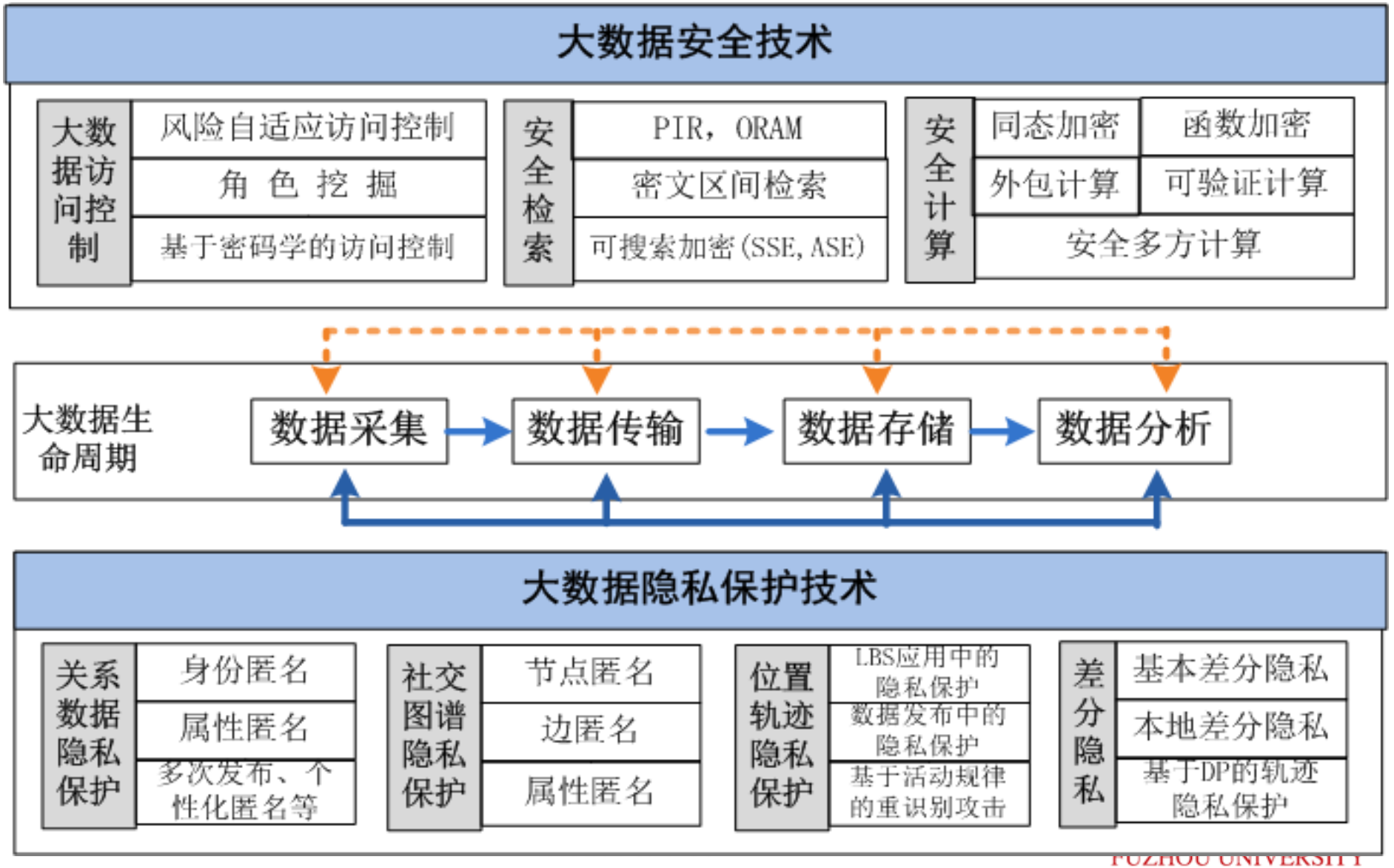
2.7 管理安全

- 管理人员的安全意识
- 管理人员的技术手段
- 安全管理规章制度
- 安全防范体系的建设

管理安全 =?= 社工安全



2.8 大数据安全技术与大数据隐私保护-冯登国



谢谢大家，一起交流学习！

QQ：10068 0 2383