**Database Security and Backups**

1. **Technical Safeguards – Access Control技术保障-访问控制**
2. **Access Control Policy (People and Procedures)**

* **A high level set of rules to grant, revoke and or deny access to the database用于授予、撤销或拒绝对数据库的访问的高级规则集**

1. **Access Control Model (Procedure)**

* **The model is the formalised policy of the rules**

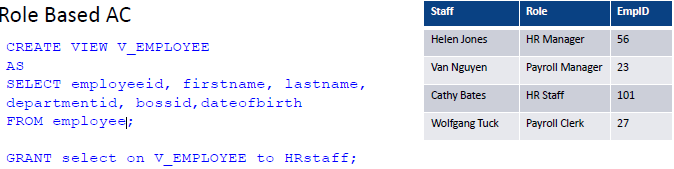
1. **Access Control Mechanism (Data and Technical)**

* **The mechanism is the means to enforce the policy**

1. **Policy content example: Only HR & Payroll managers should be able see the salary of employees. Only HR staff should be able to see an employee’s date of birth**
2. **Model:**

* **Everybody who is a HR Manager or Payroll Manager will be able to see the employee table, all other job roles such as HR Staff, or Payroll Clerk will have to access the employee table via a view which omits the salary information. Only HR staff should be able to see an employees date of birth**

**HR经理或Payroll经理可以查看员工表，其他所有工作角色，如HR Staff或Payroll Clerk，都必须通过忽略工资信息的视图访问员工表。只有人力资源员工应该能够看到员工的出生日期**

* **Mechanism: Role Based AC**
* ****

1. **Access Control Types**
2. **Discretionary Access Control - DAC自主存取控制**

* **Based on the identity of the user requesting access**
* **Explicitly states which user (subject) can perform which action (action) on which resource (object)**

**显式声明哪个用户(主体)可以对哪个资源(对象)执行哪个动作(动作)**

* **DAC mechanism controls are defined by user identification with supplied credentials during authentication**

**DAC机制控制由在身份验证期间使用提供的凭据的用户标识定义**

* **Data owners (or any users authorised to control data) can define access permissions for specific users or groups of users**

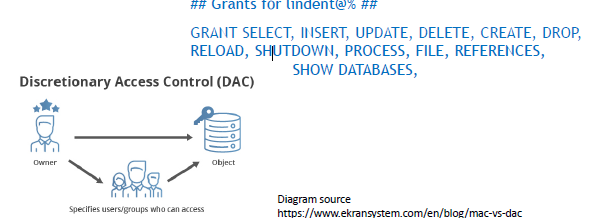
**数据所有者(或任何被授权控制数据的用户)可以为特定用户或用户组定义访问权限**

* **Authorisation is triple:**
* **Subject (User)**
* **Object (Table)**
* **Action (DML, DDL, DQL)**
* **Types of DAC**
* **Authorisation Table授权表**
* **Access Control List**
* **Capability (Owner determines access rights to the objects they own)**
* **DAC is used in UNIX, Windows, Linux, and many other network operating systems.**
* **A user may give access to their file or directory to other users or groups. The user decides on the type of control (read/write/execute…)**

**用户可以将对其文件或目录的访问权授予其他用户或组。用户决定控件的类型(读/写/执行…)**

* ****
* **DBA (or sysadmin) could perform the following types of discretionary access control**
* **Control who can create databases**
* **Prevent unauthorised users from registering user-defined routines**

**防止未经授权的用户注册用户定义例程**

* **Example:**
* ****

1. **Mandatory Access Control (MAC)**

* **Single Sign On**
* **Active Directory**

1. **Role Based Access Control (RBAC)**

* **Unix / Linux / Mac Groups**

1. **Examples (military systems)**

* **An individual data owner does not decide who has a top-secret clearance**
* **The owner of an object cannot change the classification of an object from top-secret to secret对象的所有者不能将对象的分类从最高机密更改为机密**

1. **Technical Safeguard – Firewalls**
2. **Protective layer between your LAN and the WAN / Internet**
3. **Software or dedicated hardware-software unit selectively blocks or allows data packets软件或专用的硬件-软件单元有选择地阻塞或允许数据包**
4. **All network traffic is quarantined and authenticated隔离和验证所有网络流量**
5. **Often several layers and types of firewall**
6. **DMZ – Demilitarized Zone**
7. **Data Safeguard - Encryption资料保安-加密**
8. **Encryption turns “clear text” into “\*k4#h2nsk7”**
9. **Involves very big prime number calculations used to scramble clear text**

**涉及到非常大的素数计算用来打乱明文**

* **Then “Salting” adding a byte or two to the encrypted string**

**然后" salt "在加密的字符串中添加一个或两个字节**

1. **Encryption does not hide data - it masks data**
2. **Public Key and a Private Key**

* **Public key is broadcast**
* **Private key is required to unencrypt**

1. **A encrypts sensitive information using B's public key and sends it across. B can only access that information and decrypt it using their corresponding private key**

**A使用B的公钥加密敏感信息并发送出去。B只能访问该信息并使用其对应的私钥对其进行解密**

* ****

1. **Data Safeguards – What is a Backup?**
2. **A backup is a copy of your data**

* **there are several types of backup**

1. **If data becomes corrupted or deleted or held to ransom it can be restored from the backup copy**

**如果数据损坏或被删除或被扣押，可以从备份副本中恢复**

1. **A backup and recovery strategy is needed**

* **To plan how data is backed up**
* **To plan how it will be recovered**

1. **Backups protect data from …**

* **Human error**
* **e.g. accidental drop or delete**
* **Hardware or software malfunction**
* **bug in application**
* **hard drive (failure or corruption)**
* **CPU**
* **Memory**

1. **Back-ups protection**

* **Backups could protect against**
* **malicious activity – security compromise恶意活动-安全妥协**
* **server, database, application**
* **natural or man made disasters**
* **consider the scale of the damages想想损失的规模**
* **Backups help comply with**
* **government regulation**
* **historical archiving rules**
* **Metadata collection (AUS)**
* **Privacy Rules**

1. **Categories of Failure**
2. **Failures can be divided into the following categories:**

* **Statement failure**
* **Syntactically incorrect**
* **User Process failure**
* **The process doing the work fails (errors, dies)**
* **Network failure**
* **Network failure between the user and the database**
* **User error**
* **User accidentally drops the rows, table, database**

**用户不小心删除了行、表、数据库**

* **Memory failure**
* **Memory fails, becomes corrupt记忆失效，变得腐朽**
* **Media Failure**
* **Disk failure, corruption, deletion**

1. **Types of Backups**
2. **Backups – Physical vs. Logical**

* **Physical**
* **Raw copies of files and directories**
* **Suitable for large databases that need fast recovery**
* **Database is preferably offline (“cold” backup) when backup occurs**
* **MySQL Enterprise automatically handles file locking, so database is not wholly 完全offline**
* **Backup = exact copies of the database directories and files**
* **Backup should include logs**
* **Backup is only portable to machines with a similar configuration**

**备份只能移植到具有类似配置的机器上**

* **To restore**
* **shut down DBMS**
* **copy backup over current structure on disk**
* **Logical**
* **Backup completed through SQL queries**
* **Slower than physical**
* **SQL SELECTs rather than OS copy**
* **Output is larger than physical**
* **Doesn’t include log or config files**
* **Machine independent**
* **Server is available during the backup**
* **In MySQL can use the backup using**
* **Mysqldump**
* **SELECT … INTO OUTFILE**
* **To restore**
* **use mysqlimport, or LOAD DATA INFILE within the mysql client**

1. **Backups Offline vs. Online**

* **Online (LIVE) or HOT**
* **Backups occur when the database is “live”**
* **Clients don’t realise a backup is in progress**
* **Need to have appropriate locking to ensure integrity of data**
* **No downtime or outage**
* **Physical and Logical backups**
* **Offline (Shutdown) COLD**
* **Backups occur when the database is stopped**
* **Simpler to perform**
* **Offline backup is preferable, but not available in all situations,**
* **e.g. applications without downtime**
* **Physical backups only**

1. **Backups Full vs. Incremental**

* **Full backup**
* **A full backup is where the complete database is backed up**
* **Physical (online or offline)**
* **Logical (online)**
* **It includes everything you need to get the database operational in the event of a failure它包括在发生故障时使数据库正常运行所需的一切**
* **Incremental Backup**
* **Only the changes since last backup are backed up**
* **For most databases this means only backup log files**
* **To restore:**
* **stop the database,**
* **copy backed up log files to disk,**
* **start the database,**
* **tell it to redo the log files**

1. **Backup Strategy**

* **Backup strategy is usually a combination of full and incremental backups**
* **weekly full backup**
* **weekday incremental backup**
* **Conduct backups when database load is low**
* **If you replicate the database, use the mirror database for backups to negate any performance concerns with the main database**

**如果复制数据库，则使用镜像数据库进行备份，以消除与主数据库有关的任何性能问题**

* **TEST your backup before you NEED your backup!**

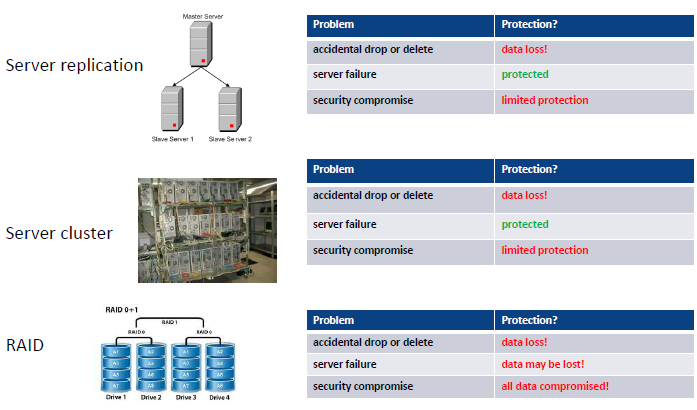
1. **Offsite Backup**

* **Motivation: hackers could still potentially get into your backups if they’re connected to your network**
* **Offsite means company backups are not stored in the organisation’s building**
* **Enables disaster recovery and business continuity**
* **Must be at remote site (e.g. ASIC require 100 km away)**
* **Backup tapes transported to underground vault备份磁带被运送到地下仓库**
* **NAB Knox City vault (15 feet silicon wall)**
* **Remote mirror database maintained via replication**

**通过复制维护的远程镜像数据库**

* **Telstra Data Centres (Melbourne and Sydney)**
* **Backup to Cloud**

1. **Other ways to reduce risk of data loss**
2. **Other ways to reduce risk of data loss**

* ****

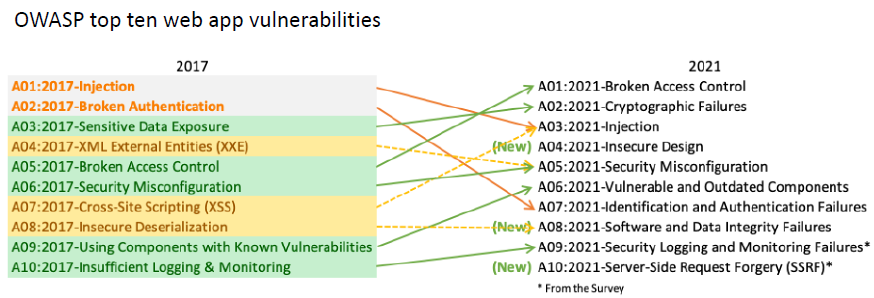
1. **Database Hardening - checklist数据库加固-检查项**

* **DB Physical Hardening**
* **harder to get to the server room**
* **Firewalls for DB Servers**
* **Database Software; App / Web Server and App Code**
* **regularly patched, constant checking for vulnerabilities**

**定期修补，不断检查漏洞**

* **Client Workstations / Browsers客户端工作站/浏览器**
* **least privilege rule最小权限原则**
* **Admin SU (Super User) accounts, permissions and passwords**
* **User roles, permissions, passwords and reporting**
* **Change Management**
* **Auditing**
* **Backup and Recovery**

1. **Web security**

* ****
* 

1. **Protecting against SQL injection防止SQL注入**

* **SQL Injection attacks**
* **a technique used to exploit web applications that use user input within database queries**

**一种用于利用在数据库查询中使用用户输入的web应用程序的技术**

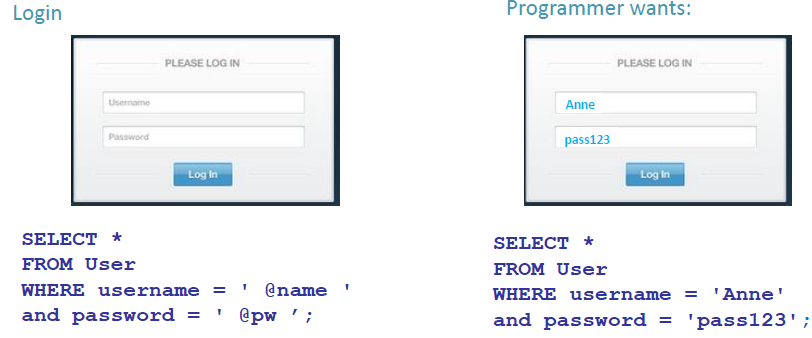
* **malicious code is entered into a data entry field in such a way that it becomes part of SQL commands that are run against the database**

**恶意代码以某种方式进入数据输入字段，使其成为针对数据库运行的SQL命令的一部分**

* **How to prevent:**
* **sanitize user inputs**
* **pass inputs as parameters to a stored procedure, rather than directly building the SQL string in the code**

**将输入作为参数传递给存储过程，而不是直接在代码中构建SQL字符串**

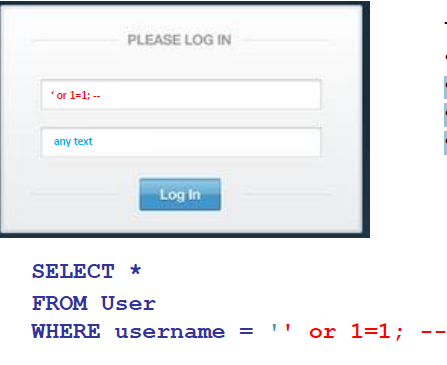
1. **SQL injection SQL注入**

* **User inputs are used to form an SQL statement**
* ****

1. **SQL injection: malicious input SQL注入:恶意输入**

* **Text entered in @name string now**
* **closes the string**
* **adds a condition that is always true**
* **ends the SQL statement**
* **begins a comment with '- - ' to neutralise the rest of the SQL**

**以“- -”开头的注释抵消了SQL的其余部分**

* ****

1. **SQL injection: prevention**

* **Primary defences:**
* **Prepared Statements (parameterised queries)** **预备语句(参数化查询)**
* **Stored Procedures**
* **(both mean SQL is no longer 'dynamic')**
* **i.e. “escape” all user input即“转义”所有用户输入**
* **turns SQL special characters like ‘ ; -- into ordinary characters**

**将SQL特殊字符';——转换成普通字符**

* **Additional defences:**
* **Principle of Least Privilege最少特权原则**
* **don't give application accounts DBA privileges**
* **White List input validation**
* **check input is from a list of acceptable values**