第一章 课后作业

1.对于下列每种资产，分别为机密性、可用性和完整性缺失分配低、中或高影响级别。并说明理由。

a. 一个组织管理 Web 服务器上的公开信息。

b. 执法机构管理极其敏感的调查信息。

c. 金融组织管理日常行政信息（不是与隐私有关的信息）。

d. 一家承包机构用于大量采集数据的信息系统既包含敏感的、预询价阶段的合同信息，也包含日常管理信息。分别对两个数据集和整个信息系统的影响进行评价。

e. 一家电厂使用 SCADA（监控与数据采集）系统控制大型军事基地的电力分配。SCADA 系统既包含实时传感数据，也包含日常管理信息。分别对两个数据集和整个信息系统的影响进行评价。

答：

a. 对于一个在组织管理 Web 服务器上的公开信息来说，信息对于所有访问的用户来说都是授权的，而机密性是保证机密信息不被非授权的人所利用，当机密性缺失时，不会带来较大的损失，因此给机密性损失分配低影响级别、对于完整性缺失来说，要看在 Web 服务器上公开的是什么类型的信息，如果是对于单位来说比较重要的信息，例如对于学校推免研究生的信息来讲等，信息要求严格，不允许随意篡改，一经篡改，将会造成恐慌混乱，因此完整性的缺失是高影响级别。对于一些无关紧要的信息，当完整性缺失时，不会造成较大的影响，因此，完整性缺失程度为低影响级别。可用性缺失，对于公开性数据来说，只是在一定时间内无法得到这些数据，在恢复可用性后，公众还是可以得到数据信息，因此可用性缺失程度为低影响级别。

b. 对于执法机构的敏感信息来说，信息的机密性缺失程度为高影响级别，因此敏感信息只能针对特殊授权的群体开放，不可泄露。信息的完整性缺失程度也是高影响级别，因为当信息被篡改后，可能会造成误差的判断，最终导致整个系统的混乱，敏感性信息不容篡改。而对于可用性缺失来说，需要判断敏感信息的紧急性，分为中或高影响程度。

c. 对于金融组织日常管理行政信息，信息的机密性缺失程度为中影响级别，当信息泄露后不会造成特别大的影响，但是也会造成数据机密性的破坏。信息的完整性缺失程度为中影响级别，如果信息遭到篡改，行政系统会产生混乱，但可以及时纠正。信息的可行性缺失程度为低影响级别，因为每日的行政信息基本保持规律，大致相同，短时间内无法得到信息也不会产生恐慌。

d. 针对包含敏感的、预询价阶段的信息，同 b 题中的信息，信息的机密性缺失程度为高影响级别，完整性缺失程度为高影响级别，而可用性缺失要根据信息的紧急情况分为中影响级别或高影响级别。

针对日常管理信息，由于不是敏感信息，但也有具体授权的客户，所以机密性缺失程度为中影响级别，而完整性缺失程度为低影响级别，因为日常信息遭到篡改后的影响程度不大，可用性缺失程度也是低影响级别。

对于整个系统来说，取两个数据集的最高影响级别，则整个系统的完整性缺失程度为高影响级别，整体性缺失程度为高影响级别，可用性缺失为中或高影响级别。

e. 对于实时传感数据，数据并不包含敏感信息，因此信息的机密性缺失程度为高影响级别，对于完整性来说，如果实时的传感数据的准确性会产生很大的影响，则完整性缺失程度为高影响级别，如果只造成不大的损失，可以判定完整性缺失程度为中影响级别。因为数据是实时的，必须要求实时传递，可用性缺失程度为高影响级别。

对于日常管理信息，等价于 d 中的日常管理信息，信息的机密性缺失程度为中影响级别，完整性缺失程度为低影响级别，可用性缺失程度为低影响级别。

对于整个系统来说，取两个数据集的最高影响级别，则机密性缺失程度为高影响级别，完整性缺失程度为高或中影响级别，可用性缺失程度为高影响级别。

2.考虑如下允许访问资源的代码：

```
DWORD dwRet = IsAccessAllowed(…);
If(dwRet == ERROR_ACCESS_DENIED)    {
// Security check failed.
```

```
// Inform user that access is denied.
} else {
// Security check OK.
}
```

a. 解释程序中存在的安全缺陷。

b. 重写代码以避免缺陷。

提示：考虑安全缺省设置原则。

答：

a. 根据安全缺省设置原则，控制访问应当基于许可而不是排除。问题中的代码是当访问出现错误时，才拒绝用户的访问，这是基于排除的方法，应当判断只有用户请求访问许可正确时，才同意访问。

b.
```
DWORD dwRet = IsAccessAllowed(…);
If(dwRet == RIGHT_ACCESS_DENIED)  {
// Security check OK.
} else {
// Security check failed.
// Inform user that access is denied.
}
```

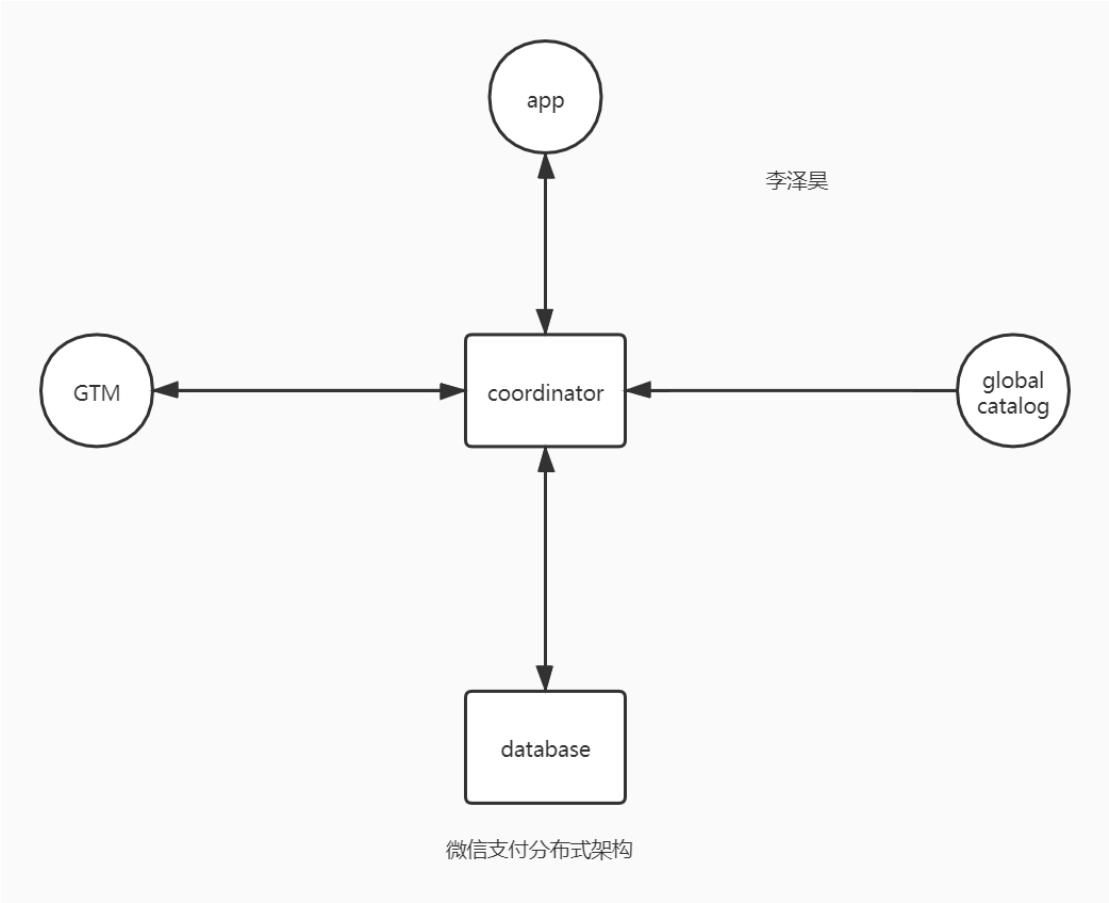
3. （1）微信支付过程有哪些环节？请画出微信支付的系统架构，并分析其存在哪些威胁？（2）支付宝支付过程有哪些环节？请画出支付宝支付的系统架构，并分析其存在哪些威胁？

对以上 2 个问题任选其一，进行讨论。

答：(1)

微信支付过程包括在支付时选择微信支付、扫描二维码、输入支付密码、完成支付。

下图是微信支付系统的系统架构：



该系统架构是一个分布式系统，当微信支付响应时，需要通过中间的 coordinator 协调器发往 GTM 请求，得到一个 GTM 信息，这个 GTM 信息必须和 coordinator 发送往各自站点的数据库，才能被正确响应。Global catalog 通过特定的权限可以协调 coordinator。

在 coordinator 发往 GTM 信息的时候可能会被篡改，信息存在着完整性缺失的可能，而对于 global catalog 存在着特殊权限，可能会存在信息的机密性缺失的可能，对于 coordinator 与数据库之间建立的链接，因为数据需要进行实时的传送，因此可能存在着信息的可用性缺失。