可修改性

- 在软件系统的生命周期中对其进行修改是客观存在的事实。
- 可修改的系统更容易演化
- 可修改性只考虑系统可能发生的变化，不需要考虑不太可能发生的变化
- 可修改性主要考虑变化的成本。

可修改性

- 可修改性用来度量修改应用程序以满足新的功能性/非功能性需求的容易程度。
- 影响很难量化
- 评估可修改性:
  - 令人信服的需求变化的影响分析。
  - 解决方案在不进行改变的情况下满足需求变化的证明。
- 降低依赖性可提高可修改性

安全性

安全性:

- **认证** — 应用程序可以验证其用户或与之通信的其他应用程序的身份。
- **授权** — 被授权的用户和应用程序具有对系统资源的访问权限 。
- **加密** — 应用程序的消息被加密。

安全性

- **完整性** — 确保消息内容在传输过程中不被修改。
- **不可否认性** — 消息的发送方有发送证明且接收者确认发送者的身份。即双方都不能否认其参与信息交换的事实。也就是说，交易不能被任意一方否认。
- **审计** — 系统跟踪内部活动并可进行重建。

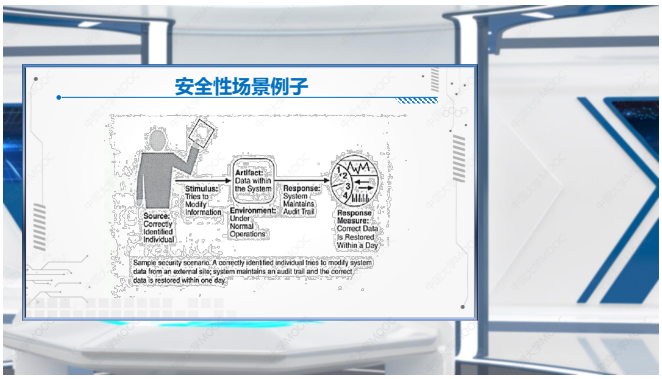
安全性

- 安全性是衡量系统向合法用户提供服务，并阻止未经授权的使用的能力。
- 破坏安全性的尝试就是攻击 ——可能是非法访问数据或服务或拒绝向合法用户提供服务。

通用安全性场景

情景组成部分	可能值
激励源	内部/外部的正确认证/未正确认证/未知的个人或系统; 授权/未授权访问有限资源/大量资源
激励	试图显示数据、改变/删除数据、访问系统服务、降低系统服务的可用性
工件	系统服务; 系统内部数据
环境	在线/离线, 连接/断开连接, 被防火墙过滤/开放
响应	认证用户; 隐藏用户身份; 阻止访问数据或服务; 允许访问数据或服务; 授予/撤回访问数据/服务的权限; 记录访问/修改或试图访问/修改数据/服务; 以不可读的格式存储数据;识别对服务的不可解释的、过度的访问，通知用户或另一个系统，并限制服务的可用性
响应度量	成功绕过安全措施所需的时间/成本/资源; 检测到攻击的概率;识别负责攻击或访问/修改数据/服务的个体的概率;在“拒绝提供服务”攻击下仍可访问的服务的比例; 恢复数据/服务;数据/服务受损及合法访问被拒绝的程度

安全性场景例子


Source:
Correctly
Identified
Individual
Stimulus:
Tries to
Modify
Information
Artifact:
Data within
the System
Environment:
Under
Normal
Operations
Response:
System
Maintains
Audit Trail
Response
Measure:
Correct Data
Is Restored
Within a Day
Sample security scenario: A correctly identified individual tries to modify system data from an external site; system maintains an audit trail and the correct data is restored within one day.