**浅谈项目管理及安全设计原则**

**摘 要**：随着信息技术的发展，软件系统建设越来越复杂，在应用中会面临各类问题，尤其是安全性问题，其暴露出的重大隐患会对整个系统的正常使用带来巨大影响。因此，做好前期设计，特别是可用性、可靠性、可维护性、可扩展性、可重用性以及安全性设计是非常必要的。文章主要论述软件系统设计的基本原则以及项目实施过程中的安全性设计原则。

**关键字**：软件设计原则、系统安全性设计、PKI体系、SSL协议

**1 引言**

现今，软件安全性已经成为一个越来越不容忽视的问题。与之对应的软件项目管理中对软件系统的设计具有比较高的要求。软件系统安全缺陷是所有常见计算机安全性问题的根源，而其安全性又是一个涉及面广泛而又复杂的课题。总有可能出现与所有已知模式完全不符合的新型安全性缺陷。因此,要从最基本的软件系统设计入手，遵循可用性、可靠性、可维护性、可扩展性、可重用性、安全性等一系列原则要求，以保护软件使其具有较高的鲁棒性，能够尽可能应对各种可能类型，包括未知类型的攻击。可以通过在设计和构建软件时运用合理的系统基本原则和安全性措施来避免软件陷入容易被攻击的状况。

**2 软件系统设计基本原则**

首先我们探讨软件系统设计的基本原则。为实现项目的友好体验、可用性、可靠性、可维护性、可扩展性、可重用性等目标，系统遵循需求牵引性原则、可扩展和易维护原则、经济性和实用性原则、先进性和成熟性原则、可靠性和稳定性原则、安全性和保密性原则等设计原则。

**（1）需求牵引性原则**

通过前期系统性需求调研，确定需要模开发的仿真模型和构建的场所环境，明确系统定位和使用人员。

**（2）可扩展和易维护原则**

在设计时应具有一定的前瞻性，充分考虑软件升级、扩容、扩充和维护的可行性。通过组件化、标准化、通用化，支持重新开发和配置应用，方便系统的纠错、改写和功能扩充。

**（3）经济性和实用性原则**

软件的设计实施尽最大可能节省项目投资，力求平台性能优良，价格合理，具有较好的性能价格比，设计面向实际，注重实效，坚持实用、经济的原则，充分合理利用现有设备和信息资源，帮助用户节省投资。

**（4）先进性和成熟性原则**

在软件设计时，将充分应用先进和成熟的技术，满足建设的要求，把科学的管理理念和先进的技术手段紧密结合起来，提出先进合理的业务流程；软件将使用先进成熟的技术手段和标准化产品，使软件具有较高性能，符合当今技术发展方向，确保软件具有较强的生命力，有长期的使用价值，符合未来的发展趋势。

**（5）可靠性和稳定性原则**

在设计时采用了可靠的技术，软件各环节具备故障分析与恢复和容错能力，并在安全体系建设、复杂环节解决方案和平台切换等各方面考虑周到、切实可行，建成的软件将安全可靠，稳定性强，把各种可能的风险降至最低。

**（6）安全性和保密性原则**

在软件设计把安全性放在首位，既考虑信息资源的充分共享，也考虑了信息的保护和隔离；软件在各个层次对访问都进行了控制，设置了严格的操作权限；并充分利用日志系统、健全的备份和恢复策略增强软件的安全性。

以上是软件系统设计基本原则的6个主要方面，如果在设计时遵循将极大提高系统的可用性、可靠性、可维护性、可扩展性、可重用性。

**3 项目实施安全性设计原则**

接下来我们详细论述项目实施安全性设计的相关原则。系统的安全需求主要来自两方面：首先是交易数据安全，系统各业务的完成主要基于因特网或局域网的传输，网络的开放性决定了其传输安全的脆弱性，需要保证数据传输的机密性、完整性；其次是网络安全，网上的公开服务器以及内部与之相连的内部服务器将不可避免的受到恶意攻击和好奇者的试探，需要保证系统强的抗攻击性。

从系统的整体安全角度来说，系统安全需要重点考虑如下几个方面的内容。

**（1）PKI体系**

在大规模、分布式网络环境中，建立系统的PKI体系，可利用公钥密码体制在身份认证、数字签名和密钥管理等多方面的优势，提供统一的身份认证、权限控制、访问控制、数字签名、数据加密、数据解密、数据完整性保护、抗抵赖性等公共的基础安全机制，保证不同安全管理域之间、不同应用业务系统之间各种安全技术的一致性、互操作性和可扩展性，对于系统服务和数据的整合和提炼、新业务的开展和实现等都有非常重要的意义。

系统的安全首先要建立一套安全应用体制，即PKI证书体制。本方案中推荐采用CFCA的普通证书的机制，遵循X.509标准，同时提供强大的扩展域定制功能，可以利用扩展域定制用户权限，以满足系统访问控制的具体需求。

**（2）CA的建立**

数字证书是PKI中最基本的概念，证书的签发者被称为CA，办公自动化业务的开展必须使用一个CA认证中心。PKI应用安全和数字证书在很多行业系统中的应用不断成熟，系统安全从应用层安全角度可以采用CFCA的安全系统。

**（3）通讯层安全**

该层次主要解决在通信过程中的数据加解密、身份认证、抗否认性和唯一性等安全通信问题。本方案中采用SSL技术和数字签名技术来解决上述安全问题。

SSL技术作为在国内外通用的在Internet中实现身份认证和数据加解密技术，经过多年的实践已经在国内众多的项目环境中得到使用，本方案中推荐使用SSL/TLS协议，128bits加密强度，CFCA站点证书（设备证书）。

数字签名技术可以保障数据在传输中的唯一性和不可否认性，在系统中可以针关键业务进行数字签名，保障关键业务的唯一性和不可否认性。

SSL（SecureSocketsLayer，安全套接层）是一种在Web服务协议（HTTP）和TCP/IP之间提供数据连接安全性的协议。由Netscape公司开发的网络安全传输协议，是目前Internet点到点之间尤其是Web浏览器与服务器之间进行安全数据通讯所采用的最主要的协议，其保证了在Internet上交换信息双方的信息安全性和可靠性。利用SSL，Web服务器还可以通过检查客户证书的内容来验证用户。典型的客户证书包含用户和证书发行机构的详细标识信息。综合使用客户证书标识和SSL，能够实现身份认证功能和防止信息篡改。SSL经过不断的完善和改进，实际上已经成为网络安全传输的标准。

1. **SSL主要功能**

SSL主要提供以下功能：

信息保密：对信息使用基于单一密钥的对称性算法进行加密。

身份认证：对通迅一方或双方使用电子证书和公钥算法进行身份确认。

信息完整：使用KeyedMAC实现信息的完整。

由于SSL具有应用面广、实施成本低、安全高效、操作简单等优点,它在多个行业系统中得到广泛的应用。

目前几乎所有的Web服务器和浏览器都具有SSL功能，但是受美国加密产品出口限制，一般加密位数只有40位，很容易被攻破，所以国内普遍采用SSL代理软件对SSL进行加强，达到128位。

SSL安全通道系统包括客户端镶嵌在浏览器中的CSP模块和SSL安全网关系统组成，浏览器通过CSP模块所提供的密码功能与服务器端安全网关使用SSL安全协议建立的128位SSL加密连接，保证业务交易的安全进行，其系统组成如下图所示：



图 1 报表引擎流程

1. **SSL安全网关的价值**

* PKI的全面支持

证书单双向的认证选择SSL网关可以配置建立加密连接时是否认证用户证书。

* 多服务，多站点证书支持

SSL网关可以建立多个服务，保护不同的应用，每个服务可以使用不同的站点证书。

* 多条证书链支持

SSL网关支持多条证书链同时存在、同时生效，即同一个SSL服务可以同时认证多家CA中心的证书用户。

* 动态黑名单支持

SSL网关可以自动到LDAP发布点获取黑名单，并动态更新，不需要重新启动服务。

* 对用户的一致性认证

通常的网关产品只是建立了一个加密连接，与应用完全无关，SSL服务可以将用户证书中的任意信息以cookie方式向后台服务器传送，应用系统无需额外接口就可以方便获取证书用户信息，即保证了用户的一次登录，又保证了应用对用户认证的一致性，安全性得到进一步保障。同时，使用SSL网关保护的多个应用系统也实现了对用户的单点登录功能，即用户使用一张证书登录所有应用系统。

* 对应用的加速

SSL服务模块高端产品采用硬件加速卡，加解密运算全部由硬件完成，效率是同等硬件环境下软件实现的10倍以上，可以彻底将应用服务器的CPU资源从繁重的加解密中解放出来，起到了对应用加速的作用。

* 多应用支持

SSL网关除了可以对B/S应用进行安全防护外，对于FTP、TELNET、SSH、远程桌面、SMTP、POP3等多种非B/S应用，具有广泛的适用性。

* 单点登录

对于某些无法修改或者无法获取证书信息从而无法实现用户一致性认证的应用，SSL网关可以实现证书与原有用户信息的映射，在应用无需任何改动的情况下自动完成系统登录，实现单点登录功能。

**（4）网络层安全**

系统安全中，除了采用安全通信和数字签名等技术外，网络层的安全技术也十分重要。在本方案中网络层的安全防护主要是通过防火墙，防病毒，入侵检测等安全技术，保障整个系统的网络层安全。

网络层安全集成主要的建设内容是网络安全基础设施的部署，包括安全区域的合理划分，为实现网络层安全而实施的防火墙、入侵检测、流量检测、完整性保护系统、防病毒网关等安全产品和安全技术。

典型的网络层安全需要考虑如下问题：

* 需要建立防火墙用以对网络各区域进行逻辑隔离。
* 需要使用VLAN划分不同网段，对关键服务器进行分组安全隔离。
* 需要建立入侵检测系统随时监视网络入侵行为，阻断入侵行为并报警。
* 需要建立全网防病毒系统，保护重要服务器和工作站不受病毒侵害，构成统一整体，但在病毒的管理方面实行分散管理，需要在Internet出口处建立防病毒网关，防御Internet病毒对系统内部的侵害。

在主干交换机实施流量检测系统，监视主干交换机上的百兆以太模块实时数据流量。

对网络设备制定安全保护策略。

**（5）系统层安全**

系统层安全是针对运行办公自动化系统的操作系统和数据库等软件平台进行安全防护，其主要采用的措施如下：

安装系统的安全补丁（Patch）。

关闭不需要的进程服务和端口。

使用漏洞扫描产品，定期进行安全扫描及时发现问题并采取补救措施。

审计系统设置配置，避免因配置不当造成的权限管理混乱。

**（6）业务安全控制**

1. **会话管理（Session）**

系统与应用服务器的会话管理结合，实现多种会话的建立和管理，让不同的会话采用统一的管理机制。以及动态负载均衡状态下的会话数据同步。同时实现会话的超时管理，有效防范避免黑客使用已经失效的会话攻击系统，同时防止垃圾会话数据占用内存，影响系统性能甚至使系统无法工作。

系统中登录的每一个客户都会有唯一Session用于保存客户在运行期内的主要信息，以供客户交易时使用，在客户退出系统时失效；同时，为避免过多的占用系统资源，以及从安全的角度考虑，系统中未使用的Session（因客户操作不当造成）在存在一定时间后会失效。Session管理包括：Session建立，Session超时处理，Session清理。

1. **表单输入校验**

对用户从表单输入的数据进行客户端（JavaScript）和服务器端双重校验，防止用户提交非法数据、以及表单数据在提交后被篡改。

1. **SQL注入过滤**

系统通过全面采用PreparedStatement方式，且将SQL和输入输出参数分开，从而以防止SQL注入攻击。

1. **脚本注入过滤**

系统为防止用户端通过页面输入html字符或javascript导致交易回显页面行为异常，交易数据返回到页面前将执行注入过滤，将关键字转换为转义符，如<script>将转换为&lt;script/&gt;，<a>将转换成&lt;a/&gt;。这样客户端浏览器不会执行注入的脚本，而只是解释为文本。

1. **关键信息加密存储**

系统对所有关键信息（如密码），都以加密成密文进行存储，防止内部人员读取关键信息明文。

1. **应用访问控制**

系统只开放提供用户访问的接口，而且通过接口只能完成系统提供的功能，有效防范黑客请求。

**（7）多种安全手段并用**

系统服务为用户可使用的USB-Key等安全工具进行业务操作，用户可以拥有多种或者一种安全工具，未来系统可以在此基础上方便的添加其他的安全工具而不需要修改所有的交易服务，大大提高了系统的可升级性、可维护性和便利性。

以上是项目实施安全性设计的基本原则，如果在安全性设计时能够遵循上述7条原则和措施，将极大提高系统的鲁棒性和安全性。

**4 综述**

综上所述，软件系统的安全性设计至关重要，本文从软件系统设计基本原则入手，对软件系统设计中的需求牵引性原则、可扩展和易维护原则、经济性和实用性原则、先进性和成熟性原则、可靠性和稳定性原则、安全性和保密性原则进行了详细论述；而后对项目实施的安全性设计原则，包括：PKI体系、CA的建立、通讯层安全、网络层安全、系统层安全、业务安全控制及多种安全手段并用原则等进行了深入探讨，希望借此能为国民经济建设中的软件项目管理及安全设计提供有益参考。

参考文献

[1] [关振胜编著](https://s.wanfangdata.com.cn/paper?q=%E4%BD%9C%E8%80%85:%22%E5%85%B3%E6%8C%AF%E8%83%9C%E7%BC%96%E8%91%97%22). 公钥基础设施PKI及其应用[M]. 电子工业出版社, 2008.

[2] 许震. SSL协议及其应用[J]. 电信快报, 2014(5), 28-31.

[3] 李雪飞, 李海峰. 软件安全性设计的分析验证要求研究[J]. [航空标准化与质量](https://sns.wanfangdata.com.cn/perio/hkbzhyzl). 2017(3), 41-45.

[4] 冯济舟, 朱婷婷. 软件安全性设计常见问题的思考[J]. 航天标准化. 2017(4), 48-50.

[5] 于志勇. 基于PKI技术的区域性网络安全认证平台建设研究[J]. 网络空间安全. 2017(11), 19-26.