试题 12 论企业内部网的安全策略

企业网络的建设是企业信息化的基础。近几年，许多企业都陆续建立了自己的企业网，并通过各种方法与 Internet 相连。网络信息安全已经成为企业信息化成功实施的关键因素。

请围绕“企业内部网的安全策略”论题，依次对以下三个方面进行论述。

1、概要叙述你参与分析和开发的内部网络以及你所担任的主要工作。

2、具体叙述在设计该系统时需要考虑的安全因素和选择安全标准的策略，以及在建立系统时所采取的综合安全措施。

3、评价你所采取的安全措施及其效果，以及其中可以改进的方面。

试题 12 解答要点

内部网（Intranet）是指利用因特网和 Web 标准和产品创建的企业内部网络。这些私有网络利用因特网和 Web 的基础设施和标准，但却通过防火墙等安全防护系统与公共因特网隔离开。公司员工可以进入因特网，但未经授权的用户却不能够进入内部网。

1、网络安全需求

而根据 ISO 7498-2 提出的 5 种安全服务，相应地提出了 Intranet 网络安全需求。主要包括身份认证、授权控制、数据加密、数据完整性以及抗抵赖性。

（1）身份认证

身份认证是授权控制的基础。身份认证必须做到准确无二义地将对方辨别出来，同时还应该提供双向的认证。即互相证明自己的身份。

在单机状态下身份认证可分为三种主要的类型：一是双方共享某个秘密信息，如用户口令；二是采用硬件设备，如编码发生器来生成一次性口令；三是根据人的生理特征，如指纹、声音来辩别身份。

而在网络状态下的身份认证更加复杂，主要是要考虑到验证身份的双方一般都是通过网络而非直接交互。目前一般采用基于对称密钥或公开密钥加密的方法，如 Kerberos，PGP。

（2）授权控制

授权控制是控制不同用户对信息资源访问权限，对授权控制的要求主要有：1）一致性，即控制没有二义性；2）统一性，对信息资源集中管理，统一贯彻安全策略；3）要求有审计功能，对所有授权记录可以核查；4）尽可能地提供细粒度的控制。

（3）数据加密

数据加密是最基本的保证安全通信的手段。目前加密技术主要有两大类：一类是基于对称密钥加密的算法，也称为私钥算法；另一类是基于非对称密钥加密的算法，也称为公钥算法。而加密手段可以分为硬件加密和软件加密法，硬件加密速度快、效率高、安全性好、成本高；软件加密成本低且灵活。密钥的管理包括密钥的产生、分发、更换等。

（4）数据完整性

数据完整性是指通过网上传输的数据应防止被修改、删除、插入、替换或重发，以保证合法用户接收和使用该数据的真实性。

（5）抗抵赖性

接收方要确保对方保证不能够抵赖收到的信息是其发出的信息，而且不是被他人冒名、篡改过的信息。通常采用的方法是电子签名。

2、网络安全设计原则

在安全策略设计时应该遵循一些合理的原则，以使其安全和保密更有保障，主要包括以下几个方面：

（1）网络信息系统安全与保密的“木桶原则”

（2）网络安全系统的整体性原则

（3）网络安全系统的有效性和实用性原则

（4）网络安全系统的“等级性”原则

（5）设计为本原则

（6）自主和可控性原则

（7）安全有价原则

3、网络信息安全设计与实施步骤

（1）确定面临的各种攻击与风险

（2）明确安全策略

- 系统的整体安全性，由应用环境和用户需求决定，包括各个安全机制的子系统的安全目标和性能指标
- 对原系统的运行造成的负荷与影响
- 便于网络管理人员进行控制、管理和配置
- 可扩展的编程接口，便于更新和升级
- 用户界面的友好性和使用方便性
- 投资总额和工程时间。

（3）建立安全模型

- 安全体制：包括安全算法库、安全信息库和用户接口界面
- 安全连接：包括全连接协议、身份验证协议、密钥分配协议等
- 网络安全传输：包括网络安全管理系统、网络安全支撑系统和网络安全传输系统等

（4）选择并实现安全服务

（5）安全产品的选型测试

从上面的分析中，我们可以得知关于企业内部网安全策略的论文的写作要点大体上包括以下几个方面：

（1）所举的企业内部网项目应结合以上五个方面的安全需求进行描述，清晰地说明其在这些方面所面临的问题，并应适当地说明该系统的应用背景与目标。

（2）文章应该结合所举的企业内部网项目的实际情况，系统地整理出要考虑和解决的安全因素，并且围绕着这些安全因素阐述所选择的安全策略与安全模型。

（3）文章应该在安全策略和安全模型的基础上，具体地展开说明所采用的措施。而且应该在这个部分的描述中，重点陈列实践的工作过程，而不要过多地列举理论知识，要充分体现出自己的项目实践经验。

（4）应对所选的技术与措施的效果进行分析，并力求实事求是，毕竟每一种都会有一定的适用范围和局限性。

（5）文章可以使用一定篇幅对解决方案的不足进行描述，并提出一些可以进一步尝试的新解决方案。