信息系统自身安全的基本要素

身份认证的作用和意义

零知识证明

身份认证的分类

基于hash函数实现口令认证的好处

基于hash函数口令验证的过程

基于数字证书的单向身份认证协议

生物认证的重要安全指标

访问控制和安全审计的含义

信息系统自身安全的要素？

身份认证，访问控制，安全审计，数据安全

身份认证是为了保证操作者的物理身份和数字身份相对应

身份认证的作用：

确保计算资源被授权的人使用

身份认证的意义：身份认证往往是许多应用系统安全保护的第一道防线，它的失败可能导致整个系统的失败，多数情况下，身份认证与访问控制和审计等应用紧密结合

零知识证明：

证明者在向验证者证明有效性的时候不产生任何知识的证明，即证明者P论证的过程中验证者V得不到任何有用的信息。

一个安全的身份认证过程至少应该满足：

1. P能证明他是P
2. 是零知识证明，V不能模仿P说他是P

身份认证的分类：

1. 所知：知道密码、口令
2. 所有：有动态口令设备，IC卡，Usb Key电子钥匙
3. 所是：独一无二的身体特征，指纹，笔迹，声音

双因素认证：123里挑两种

口令易实现、成本低、使用方便

口令验证过程：

输入终端输入明文口令加密成哈希值后，与认证系统生成的随机数提问一起加密成应答，应答通过公开信道传到认证系统，认证系统通过随机数和铭文口令的的哈希值生成应答，与传来的应答对比是否匹配

验证码可抵抗穷举攻击和dos和重放攻击

用户要及时修改管理员设定的缺省口令，定期更新口令

基于密码技术的身份认证协议有：

1. 基于对称密码的
2. 基于数字证书的单向身份认证协议

生物特征分为身体特征和行为特征（签名，声音，行走步态

生物特征识别的重要安全指标：

1. 错误接受率，把不匹配的当成匹配的概率，要低
2. 错误拒绝率，匹配的当成不能匹配的 要低

访问控制

是实现既定安全策略的系统安全技术，根据安全策略，对访问请求做出许可或者限制访问的判断，实现数据保密性和完整性的主要手段

安全审计

指对信息系统中与安全有关的活动及其相关信息进行识别、记录、存储和分析，贯穿计算安全机制实现的整个过程，通常是实现系统安全的最后一道防线

