信息安全作业 5

190110429-何为

1. “挑战应答方式”认证和 Needham-Schroeder 对称密钥认证协议的区别？模仿 Needham-Schroeder 设计一个三方通讯认证协议。

答:

区别:

（1） 网络规模不同：“挑战应答方式”认证需要在只有少量用户的封闭式网络系统中；Neadham-Schroeder 对称密钥认证协议应用于规模较大的网络系统。

（2） 是否依赖第三方：“挑战应答方式”认证只需要通信双方参与；Neadham-Schroeder 对称密钥认证协议需要一个可信第三方，称为认证服务。

（3） 加密次数: “挑战应答方式”认证只进行一次加密解密; Neadham-Schroeder 对称密钥认证协议需要多次加密解密过程。

设计:

通过对 NS 协议加以改进，避免重放攻击:

（1） A->KDC: $ID_A||ID_B||N_1$

（2） KDA->A: $E_{Ka}[K_S||ID_B||N_1||E_{Kb}[K_S||ID_A]]$

（3） A->B: $E_{Kb}[K_S||N_1||ID_A]$，在这一步验证中加入 N_1 作为时间戳，进行认证。

（4） B->A: $E_{Ks}[N_1||N_2]$，在这一步验证中，B 获得了N_1并发回 A，达成验证。

（5） A->B: $E_{Ks}[f(N_2)]$

2. 解释详细 Kerberos 认证协议过程。

答:

（1） 第一阶段：身份验证服务交换，完成身份认证，获访问 TGS 的票据。

步骤 1 为请求 TGS 票据，步骤 2 为返回 TGS 票据。

（2） 第二阶段：票据授予服务交换：获得访问应用服务器的票据。

步骤 3 为请求应用服务器票据，步骤 4 为返回应用服务器票据。

（3） 第三阶段：客户与服务器身份验证交换：获得服务。

步骤 5 为向应用服务器发起服务请求, 步骤 6 为服务器对客户机可选的身份验证。

3. 什么是数字证书，如何使用数字证书进行身份认证?

答:

数字证书是一个经过权威的、可信赖的、公正的第三方机构（即 CA 认证中心, Certificate Authority）签名的包含拥有者信息及公开密钥的文件，绑定了公钥及其持有者的真实身份。

认证过程有五步:

（1） 示证方 A 提交资料，申请证书。

（2） CA 审核 A 的资料，颁发用 CA 私钥签过名的数字证书。该数字证书包含了 A 的身份信息和 A 的公钥。由于使用了 CA 的私钥签名，因此其他人无法伪造。

（3） A 使用私钥对特定信息进行签名，连同数字证书一起发送给 B，B 为验证方。

（4） B 为了能够核实 A 的数字证书的真伪，必须先获得 CA 的公钥。

(5) B 使用 CA 的公钥对 A 的数字证书进行合法性验证，通过后获得 A 的公钥，对 A 签过名的特定信息进行认证，进而确认 A 的身份及其签名的信息。

4. 什么是 PKI，它包含那些主要功能，如何工作?

答:

PKI 是一种遵循一定标准的密钥管理基础平台，为所有网络应用提供加密和数字签名等密码服务所必需的密钥和证书管理。PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。

主要功能：用户可利用 PKI 平台提供的服务进行安全的电子交易、通信和互联网上的各种活动。

工作原理：PKI 采用数字证书技术来管理公钥，通过 CA 认证中心把用户的公钥和用户的其他标识信息捆绑在一起，在互联网上验证用户的身份。通过作为中心的公钥算法和数字证书技术、第三方的可信任机构 CA 认证中心、证书库、密钥备份及恢复、证书撤销处理、PKI 应用接口等完成工作。

5. 什么是证书链，X.509 是如何实现证书认证的?

答:

证书链是由根证书，中间证书，用户证书等组成一条完整证书信任链，是由一串数字证书链接而成。

X.509 V3 证书包括一组按预定义顺序排列的强制字段，还有可选扩展字段。通过建立 CA 目录的层次结构，证书的认证路径构成一个证书链。X.509 证书由公钥和私钥组成的密钥对而构建的。公钥和私钥能够用于加密和解密信息，验证发送者的身份和确保消息本身的安全性。