基于 NETSCAPE 的企业网信息服务安全体系的建立

吴钧　熊华平　（大庆勘探开发研究院　163712）

摘要：本文分析了网络信息服务安全的基本需求，剖析了 Netscape 的安全机制，最后就建立企业网信息服务安全体系的实施过程给出了一些建议。

关键字：信息服务　网络安全　证书　加密

一、引言

企业网安全的核心是信息的安全。为防止非法用户利用网络系统的安全缺陷进行数据的窃取、伪造和破坏，必须建立企业网信息服务安全体系。信息的安全隐患在于信息的传递和共享过程中。随着浏览器/服务器技术的成熟，这一技术已广泛应用于工作组级、部门级、专业系统级乃至整个企业网规模级的应用。作为企业网应用系统的典型代表，WEB、MAIL、NEWS 普遍采用信息共享和传递的通信方式。本文首先介绍信息服务安全的基本要求，然后结合 Netscape 安全解决方案，对建立企业网信息服务安全体系进行一些探讨。

二、企业网信息服务安全的基本要求

从安全机制的角度分析，企业网信息服务有以下安全要求：

1. **用户认证**

随着网络的增大和用户数、服务器的增多，基于两个原因，一般口令认证已经不够安全可靠。一是用户口令在传输和存储时如果不加密有可能被窃取；二是口令认证的强度很大程度取决于口令设置的好坏，由于很多用户为了便于录入和记忆，设置的口令往往很短或有规则，容易被猜测出或在输入时被人看到。改进的办法是采用 512 或 1024 比特的密钥来认证用户和服务器，用户只要记忆用于加密存储证书文件的口令即可。同一证书可用于向多个服务器进行用户认证。

2. **信息的加密存储**

为防止信息在机器内存储时被系统管理员或其他用户通过网络、操作系统等途径间接获取，对信息需要加密存储。

3. **信息的加密传输**

为防止信息在网络传输过程中被网络管理员或其他用户窃听，需对信息进行加密传输。

4. **信息的数字签名**

为防止邮件、公文等信息在生成、传输和存储过程中被伪造，可对信息进行数字签名。签名可确保传输的信息未被篡改和伪造。

5. **完备的信息授权控制**

由于信息的多样性和用户的多样性，对于较复杂的信息系统需要完备的授权规则功能支持。

6. **全局目录服务**

大型企业网有大量用户，用户标识如果不进行标准化和集中管理将使信息和网络授权很难实施。

三、Netscape 安全解决方案

通过以上信息服务的安全需求分析可以看出，要建立企业网信息服务安全体系，一方面，企业网的信息服务平台应有足够的安全支持能力；另一方面，应配之以有效的管理和系统的筹划。

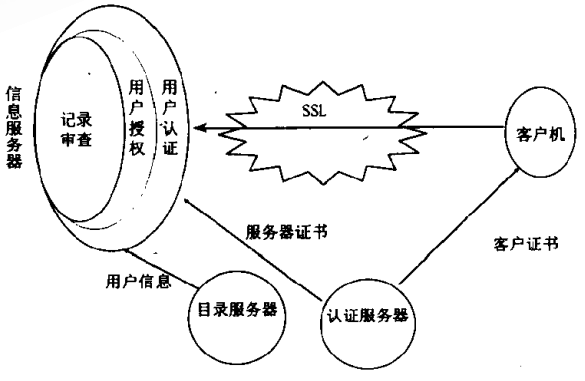

图 1　Netscape 信息安全服务解决方安示意图

Netscape Suitespot 套件以各种网络信息服务的安全需求为核心，提供了初步的一体化解决方案(如图 1 所示)，可在各种安全等级的网络上实现各种安全等级的网络信息服务。

1.信息加密机制

防止数据在传输过程中泄密的措施是采取数据加密。Netscape 的信息加密机制体现在安全端口协议，内部嵌入了 RSA 公开密钥加密系统。其基本原理是通过公开密钥、私有密钥来完成信息的加密和解密，即发送端采用公开密钥加密信息，接收端采用私有密钥解密(如图 2 所示)。

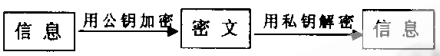

图 2 加密原理图

数字签名是通过一定的算法，把要发送的信息提取成固定长度的校验序列，并对该序列用私有密钥加密，连同信息一起发送。接受方用接收到的信息产生的校验序列与用公开密钥解密的校验序列比较，如相同，则证明发送方未被仿冒且信息未被篡改。该方法可用于公文批示。

2.证书认证

尽管公开密钥提供了一个验证用户的方法，但并不能保证公开密钥事实上真正属于声称的所有者。因此，公开密钥必须由一个权威的验证机关所认证。证书是一个数字文件，用于为个人、计算机系统或组织作身份和公开密钥所有者的担保。证书由证书认证机构(CA)发放，CA 负责在发证前验证申请者的身份及公开密钥所有权。Netscape 识别符合 X.509 国际标准的证书格式。证书由证书数据和发放证书的 CA 签名数据两部分组成，证书数据的主要内容是：

(1)证书格式版本号

(2)证书序列号

(3)CA 的签名算法

(4)CA 标识名(distinguished name)，格式符合 X.500 标准

(5)证书有效日期

(6) 证书持有者标识

(7)公钥信息

通过证书认证身份是建立加密传输的基础和前提。

3.加密传输

Netscape 自主开发并已成为工业标准的安全端口层(SSL)协议可保证网络环境下的信息传输的保密性、完整性和可靠的用户认证。

SSL 的核心技术是利用证书提供的公开密钥协商会话密钥后进行对称式信息加密传输。SSL 运行于 TCP/IP 协议之上和 HTTP、FTP 等应用协议之下，以保证各种网络应用的安全(如图 3 所示)。

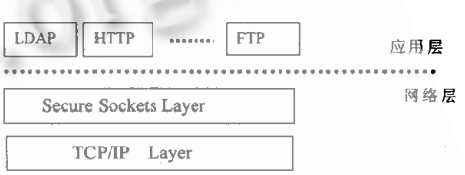

图 3 协议层次图

下面是对 SSL 会话建立步骤的简要描述：

(1) 客户端请求连接。

(2) 服务器发送一个已签名的证书给客户端。

(3) 客户端检查证书发放 CA 是否为其所信任，如果是，比较证书的标识(域名、公钥)是否与实际相符，如相符，客户端建议加密算法、密钥类型。

(4) 服务器接受加密算法、密钥类型。

(5) 客户端生成一个会话密钥，用服务器的公钥进行加密发送。

(6) 服务器接受会话密钥。

(7) 加密通信开始。

Netscape 的 Web、Mail、News 等各项信息服务均支持基于 SSL 的用户认证加密传输。

4.授权与审查

Netscape 支持多条件规则授权，如域名、IP 地址、时间、目录等，并可定义多种事件的记录，以生成审查报告。

5.目录服务

目录服务实现用户信息的集中管理和查询。NETSCAPE 采用工业标准的 LDAP(轻量目录介入协议)，具有开放性和标准化的优点。由于 Suitespot 的大多数服务器(包括使用本地用户管理的服务器)采用了目录数据标准格式，因此可以向全局目录服务平滑过渡。

四、Netscape 信息服务安全体系的实施

1. 建立认证服务器

在企业网最上层信息中心建立顶级认证服务器(CA),负责证书的管理。与证书管理相关的任务包括接受各种证书请求(服务器、客户、邮件、CA)、证书归档和备份、证书注销、保证证书服务器自身的安全、确定证书的发放政策、确定证书机关的授权和代理、制定名字空间的标准、明确用户的使用责任、证书发放的审查等。在证书管理中,各系统管理员职责如下:

·系统管理员:负责配置和管理证书服务器。

·证书发放员:负责证书申请检查和发放。

·其他服务器管理员:为所管理的服务器申请和使用证书。

·最终客户:个人证书的请求、保管、使用。

2. 建立信息中心目录服务器

建立信息中心目录服务器的目的是利用目录服务器统一管理若干邮件服务器、WEB 服务器等的用户信息。为保证目录服务器的可靠性和保密性,应制定必要的名字规范和合理的目录管理规则。下面是有关角色职责:

·系统管理员:启动目录服务器,增加、删除目录数据库,管理权限,管理配置文件等。

·子目录管理员:负责某个 OU(下级单位)的信息管理。

·目录应用开发人员:负责目录服务界面定制、属性增加等增值开发。

3. 多级认证和目录服务

根据企业网的规模,建立多级认证机构和目录服务机构(如图 4 所示)。采用多级 CA 授权和多级目录服务器复制技术,确保在系统规模扩大的同时保证系统的保密性和可靠性。

4. 安全策略的考虑

尽管 Netscape 提供了全面的安全功能,但对于不同安全级别的信息和网络环境应选择不同安全级别的方案。

·只有在不安全的网络通信路径中才须使用加密传输和认证。

·对用户可定义安全级别组,统一授权,便于管理。

·对不同安全级别信息尽量放在不同目录下,使授权规则定义尽可能简单,减少漏洞。

·对于部门内信息共享,如果属于单独的子网或网段,为便于用户使用,在信息安全级别不高的情况下,只用域名、时间作为介入控制条件即可。

·保密信息尽量与公用信息放在不同的服务器中,对保密要求高的服务器设置详细存取记录。此外还应堵塞网络操作系统环境下的其他信息泄露途径。

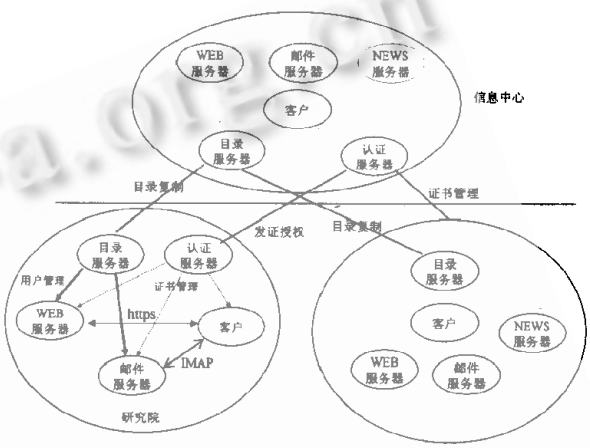

图 4 多级认证与多级目录服务

五、结束语

今天,企业网已经成为企业的最重要的基础设施,并将为国民经济现代化发挥越来越重要的作用。如何利用国内外最先进的技术或产品建立企业网信息服务安全体系,将直接影响企业网信息系统的保密性、可靠性、易维护性、易使用性。同时,合理的规划和严格的管理制度也将是建立企业网信息服务安全体系成功的关键。

参考文献

[1] Netscape Certificate Server Administrator's Guide, 1997

[2] Carl A. Sunshine, Computer Network Architecture and Protocols, Plenum Press, New York, 1989

[3] Netscape directory Server Administrator's Guide, 1997

[4] 胡曹元,基于分布式目录服务的电子邮件安全技术,《计算机工程与应用》1997 年第 3 期

(来稿时间:1998 年 2 月)