分层体系应用安全认证机制的研究和实现

王茯　徐进（北京理工大学计算机科学工程系　100081）

摘要：本文围绕Internet环境下分层体系结构事务处理系统的安全认证机构，讨论关于建立单一认证机制所带来的局限性和不可回避的问题。提出了适合分布式计算机环境的、可扩展的分层体系应用的安全认证机制。

关键词：分层体系结构的应用　安全认证机制

随着互联网在世界范围的普及，依赖Internet的分层体系结构应用已经形成主流趋势，越来越多的人们认识到，Internet不仅是信息的平台，而且也是极为便利的事务处理应用平台。分层体系结构是在Internet环境下事务处理系统的典型体系结构，在分层体系结构的应用中建立单一的认证机构来保证信息的安全性，有着很大的局限性和不可回避的问题。本文围绕在Internet上的分层体系应用特点，讨论关于建立单一认证机制所带来的问题，提出了适合分布式计算机环境的、可扩展的分层体系应用框架的安全认证机制。

1　层体系结构应用的安全认证问题

依赖于Internet的分层体系应用具有如下特征：

(1) 分布在网上不同地域的事务性应用，具有典型的多层上下级关系。例如，上级政府向下级政府；上级总销售商对下级分销商；会员中心和各区域分会，等等。

(2) 事务信息是分级管理和存放的，但实际资源是分级共享的，各级应用系统对共享的资源拥有不同的使用权限。例如，中央，省，市、县各级政府对信息存在自上而下的控制使用权，而自下而上的信息使用权通常是受限的。

(3) 不同级别的应用事务结点经常需要添加，存在扩充的需求。

显然Internet所提供的网络资源共享的灵活性以及分布协同工作服务方式，为分层的事务应用带来极大的方便，但所面临的安全问题也是异常严峻的。在事务信息传送中，如何保证信息在通信过程中不被更改，怎样控制数据在通信期间不被执行非法操作；又如何保证通信双方彼此的身份，不是假冒的用户以获得非法的服务。解决安全问题通常的技术无非是两项：数据加密和安全认证。

基于上述分层体系应用的特征，采用单一的认证机构为所有的结点和WEB服务器发放证书，来实现分层的、不同级别控制是很困难的，并且难于实现网络的结点扩充。因此根据分层结构的信息分布以及级别需求特征，我们提出了基于X.509树型公钥签发模式和树型公钥分配构架。

2　分层体系结构应用的安全认证机制

认证体系的主要目的是验证信息的发送方和接收方的真实身份，以及验证信息在传输过程中未被窜改、拦截和监视。基于Internet的安全认证系统一般采用非对称密码体制的公钥体系结构PKI（Public Key Infrastructure）来实现。在PKI中，用户使用证书来证明自己的身份。认证机构CA（Certification Authority）事先为用户生成一对公钥和私钥，并为用户发放证书，包含用户的公钥、用户名称、证书版本号、证书序列号、CA数字签名、有效期限等。发送方用自己的私钥加密自己传送的信息，接收方通过发送方的用户证书确认发送方的身份，获取发送方的公钥。认证机构CA将公钥预先发送给每一个用户，通过数字签名来保证用户

的证书的真实性。

分层体系结构的应用需要多级的 CA，高级别用户和低级别用户之间的信息访问，不同级别 CA 认证的用户之间的信息访问，都必须同时提供证书链及交叉认证服务。

在用户数量大，分属不同地域，且需要不同权限的应用中，可构造的安全认证体系 CA 层次管理，如图 1 所示。

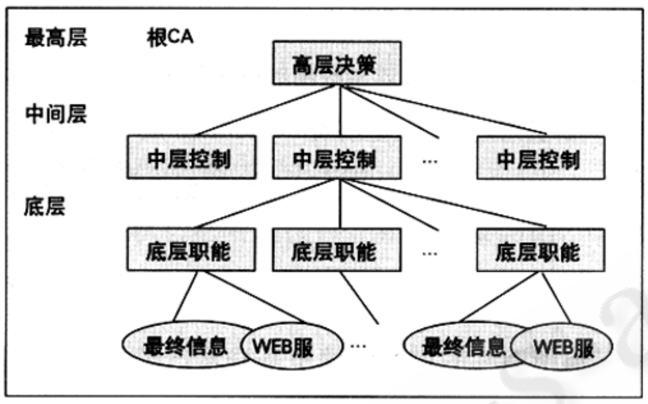

图 1　CA 的分层体系结构图

顶层根 CA 是认证系统中的最高认证机构，享有最高权限，它将为下层 CA 签发 CA 间证书，还包括交叉认证证书。根 CA 的安全着重于物理安全、网络安全和主机安全。

中层 CA 为控制机构，其功能是向下一级 CA 发放 CA 证书，并传递根 CA 的信用权威，中层 CA 的物理安全、网络安全及主机安全接近根 CA 的需求。

底层 CA 为职能机构，其功能是面向最终用户和 WEB 服务器签发证书，发放证书的数量比较大，签发的证书种类也比较多。

在分层管理的认证方案中，根 CA 和中间层 CA 与外部的联系不多，可隔离 CA 私钥管理、证书签发、内部的数据等安全性要求高的部分，不与 Internet 相连。这样可确保不受外部攻击。与外界进行信息通信底层 CA 与 Internet 相连，它既要为用户签发证书，又要支持用户对证书撤销表的查询，对实时性、可操作性要求较高，因而受外界攻击的机会较多。

3　分层体系应用认证机制的实现技术

3.1 分层系统中的公钥链和证书链

在分层结构的 CA 体系统中，各级 CA 和最终用户都拥有一个证书链和一个公钥链。证书链和公钥链分别记载了从根 CA 到该用户的各级 CA 的证书和公钥。

定义：

PK_i，为各层的 CA 公钥,(其中 i=1,2,3,... n)；

SK_j，为各层的私钥，(其中 j=1,2,3,... n)；

C_m，为中间各层所得到的上层所授证书（m=1,2,3,... k)；

C_{root}，根 CA 自签发的证书；

C_{object}，为底层 CA 为最终用户和 WEB 服务器发放的证书。

证书链和公钥链的生成算法如下：

(1) 根 CA 为自已生成 PK_i 和 SK_i（i=0）并自签发证书 C_{root}，产生的根 CA 的公钥链和证书链为 $\{PK_i,C_i\}|$(其中 i=0)。

(2) 各层 CA 为下层生成 PK_{i+1} 和 SK_{i+1}，为下层 CA 签发证书 C_m(m!=0)，并发送本层 CA 的公钥链和证书链。每层产生的公钥链和证书链为 $\{PK_i,C_m\}|$(其中 i||i+1||i+2||...||i+n-1，m||m+1||m+2||...||m+k-1)。

(3) 底层的 CA 生成最终用户和 WEB 服务器的 PK_{i+n}、SK_{m+k}，并签发证书，同时向最终用户和 WEB 服务器发送公钥链和私钥链，最终用户和 WEB 服务器的公钥链和证书链为 $\{PK_i,C_m\}|$(其中 i||i+1||i+2||...||i+n，m||m+1||m+2||...||m+k)。

3.2 分层系统中的 CA 交叉认证

在分层的认证体系中，不同 CA 认证的用户存在着信息交换的需求，他们之间的信任关系需要通过交叉认证来进行。交叉认证是在层次间建立关系后，互相颁发交叉认证书，并在往来的两个非同一认证 CA 签发证书的用户之间，必须先交换交叉证书，该交叉证书是用自已的私钥对应对方的公钥签名加密后生成的。

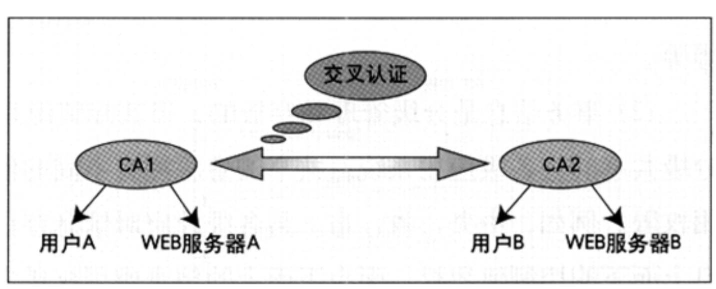

图 2　CA 间的交叉认证

如图 2 所示，用户 A、B 和 WEB 服务器 A、B 的证书是分别由 CA1、CA2 所签发的，由于用户 A 和 WEB 服务器 A 都拥有 CA1 的公钥，用户 A 访问 WEB

服务器A，只需出示自己的证书链即可以被验证。然而用户A和WEB服务器B由不同的CA签发证书，用户A想要访问WEB服务器B，必须先下载CA2为CA1发放的交叉认证证书。并把该证书放到自己的证书链中，既可象用户B一样访问WEB服务器B了。WEB服务器B通过交叉认证证书获取CA1的公钥，从而验证用户A的身份。

3.3 各级CA的信任控制

在分层体系应用中存在多个CA，CA所认证的用户对信息享有不同的权限，因而在所有CA之间建立全面的信任是不合适的，需要采取相应措施限制CA之间的信任程度。CA之间的信任关系应与CA认证的各级用户的权限相匹配。对于层次结构的认证系统，应使用层次型的网络控制方式。

约束CA之间信任关系共有三种方式：路径长度(path length)，名称(name)和政策(policy)。

(1) 路径长度约束，在层次型交叉认证中，路径长度约束通过路径长度来控制子CA数目的增加。

(2) 名称约束，在层次型交叉认证中，名称约束通过限制DN(区域名称)达到限制基于DN的子CA和其用户的增加。

(3) 政策约束，政策约束仅用于限定对其他CA中用户的信任，这些用户的证书中包含某种政策域值。

3.4 根CA的证书更新及验证路径

根CA的证书的是由自己签发的，它生成公钥私钥对，并将公钥和加密证书存放在证书数据库中以备查询。

到期的根CA的证书，或由某种原因被破坏CA的证书，将生成一个新的公钥私钥对来替换根CA现有的公钥私钥对。

更新根CA密钥时，需要重新自签发下面的三个CA证书：

(1) 新私钥对旧公钥签名证书：根CA用新CA签名私钥，对旧CA验证公钥签名，生成自签发的CA证书。该证书允许新CA签名私钥，并使创建的用户能够验证由旧CA签名私钥所签发的证书。

(2) 旧私钥对新公钥签名证书：根CA用旧CA签名私钥，对新CA验证公钥签名，生成自签发CA证书。该证书允许旧CA签名私钥，并使创建的用户能够验证由新CA签名密钥所签发的证书。

(3) 新私钥对新公钥签名证书：根CA用新CA签名私钥，对新CA验证公钥签名，生成自签发的CA证书。该证书允许新CA签名私钥，并使创建的用户能够相互验证对方的证书，而无需验证内部交叉认证链，该交叉认证链的起始，由旧自签发CA证书来确定。

认证系统中的每个用户都将保存一个公钥链和一个证书链。公钥链和证书链保存从根CA到该用户的各层CA的公钥和证书。根CA的密钥更新后，各个用户的公钥链和证书链也必须同时更新。包括子CA的公钥链和证书链和最底层CA为最终用户签发的公钥链和证书链。

完成新用户证书申请或完成密钥恢复后，下载最新的CA的证书，以保存用户证书链里的证书链CA信任锚。

验证证书通过证书链实现的方法分两种情况：当一个或多个CA密钥更新时，验证用户证书是从证书链的CA信任锚开始，经过自签发的CA证书再到目标证书的过程。如果更新时只是为验证一个来自被交叉认证的CA的证书，则验证旧用户证书验证是从旧CA信任锚开始，经过自签发CA证书，再经过交叉认证证书，最后到达目标证书。

4 认证体系的通信方案

目前电子商务中最常采用的基于证书的安全通信协议是套接字协议SSL（Secure Socket Layer Portocol）和安全电子交换协议SET（Secure Electronic Transaction)。在分层体系应用的认证体系中，仍可用已经成熟的安全协议来实现用户浏览器与WEB服务器间的安全通信。

SSL用于Netscape浏览器中，随着WEB浏览器技术的发展，SSL已成为浏览器和服务器的主要标准之一。SSL协议的主要目标是在两个通信应用之间提供私有性和可靠性。SET安全电子交换协议是在开放网络下的卡支付安全协议，它采用公开密钥体制PKI和X.509电子证书标准，通过相应软件、电子证书、数字签名和加密技术，在电子交易环节上提供信任度。SET的证书格式比较特殊，虽然也遵循X.509标准，但它主要是由Visa和MasterCard开发并按信用卡支付业务，而SET支付方式和认证结构适应于卡支付，对其他支付方式是有所限制的。

SSL和SET除了都采用RSA公钥算法以外，其他技术方面没有太多相似之处。RSA在二者中也被用来实现不同的安全目标。SET是一个多方的报文协议，它定

义了银行、商家、持卡人之间必需的报文规范。SSL 只是简单地在两方间建立安全连接。SSL 是面向连接的，而 SET 允许各方之间的报文交换不是实时的。SET 报文能够在银行内部网或者其他网络上传输，而依托 SSL 的卡支付系统只能与 WEB 浏览器捆绑在一起。

在分层体系应用中，传送的数据主要是各级用户浏览器与 WEB 服务器之间的信息传递。主要的安全问题是保证传输信息在 Internet 网上的安全性。因而采用 SSL 协议来实现浏览器和 WEB 服务器间的安全通信简便易行，从性价比上更为合适。

5 总结

本文主要讨论了分层体系应用安全认证机制的 CA 层次结构，CA 的证书链和公钥链、CA 的交叉认证、各级 CA 的信任关系、根 CA 的更新，并借鉴电子商务领域中已经成熟的通信途径，选用 SSL 协议实现用户浏览器与 WEB 服务器间的安全通信。该方案在国防信息系统项目研究中得到实现，并广泛适用于分层体系应用的 Internet 网上事务及信息系统中。■

参考文献

1 *陈凡、许先斌，SET协议的分析与改进措施，计算机应用与研究 2000 年 06 期。*

2 *陈飞，Internet 信息安全技术概述，江西通信科技 1999 年 04 期。*

3 *张军、颜凯，轻度目录访问协议的分析，计算机应用 1999 年 10 期。*

4 *Anonymity Maximum Security, Copyright 1997 by Sams.net Publishing。*

5 *Chris Hare, Karanjit Siyan, Internet Firewalls and Network Security, Copyright 1996 by New Riders Publishing。*