基于生物特征和 XML 的 C/R 认证方案①

A C/R Authentication Scheme Based on Biometric Certificate and XML

刘高嵩　曾小能　(中南大学 信息科学与工程学院 湖南 长沙 410075)

摘　要： 生物特征认证技术是利用人的生物特征进行身份认证，作为一种准确、快速和高效的身份认证方法越来越广泛地应用于各种需要身份认证的领域。在身份认证体系中，C/R 由于其简易的工作机制，使其得到广泛的应用。同时鉴于 XML 的开发性、结构性、可移植性，使其成为数据交换的标准格式；本文最终提出了一种基于 XML 和挑战/应答的生物特征认证的新方案。

关键词： 挑战/应答 生物认证 生物证书 XML

1　引言

身份认证是安全系统中的第一道关卡，用户在访问安全系统之前，首先经过身份认证系统识别身份，然后访问监控器根据用户的身份和授权数据库决定用户是否能够访问某个资源。一旦身份认证系统被攻破，那么系统的所有安全措施将形同虚设。因此加强身份认证理论及其应用的研究是一个非常重要的课题。

现在一般的身份认证系统是以用户的口令来保护密钥，但采用这样方法，存在很多缺点。例如，口令难以记忆、容易被黑客通过各种方法破译等，从而造成网络安全威胁。因此，在网络安全要求很高或者某些特殊场合需要其他方法来保护密钥。

本文借鉴 C/R 的安全服务框架思想，提出并设计了一套基于生物特征和 XML 的安全认证方案，用来提供相关安全服务，以应用于各种使用生物认证服务的场合。

2　挑战/应答身份认证机制分析

挑战/应答认证机制是一种一次性口令认证机制；每个用户都持有相应的挑战/应答令牌、令牌内置种子密钥和加密算法。

用户要求登录时，服务器随机生成一个挑战数(Challenge)，用户将该挑战数手工输入到挑战/应答令牌中，挑战/应答令牌利用内置的种子密钥和加密算法对其计算出相应的应答数(Response) 。用户将该应答数手工输入到主机再上传给服务器，服务器根据该用户存储的种子密钥和加密算法计算出应答数并与用户上传的应答数进行比较。该方法可以保证很高的安全性，是一种非常可靠有效的认证方法。但该方案直接应用在网络环境下还存在一些缺陷：用户需多次手工输入数据，易造成较多的输入失误，使用起来十分不便；用户的身份标志直接在网络上明文传输，攻击者可很容易地截获它，留下了安全隐患；令牌携带不方便等等[1]。

3　生物认证技术

生物认证是利用人的生物特征，如指纹、虹膜、语音等，进行身份认证的一种手段，是对人进行身份认证最根本的手段。随着计算机技术的发展和生物识别算法的不断改进，生物特征认证技术作为一种准确、快速和高效的身份认证方法正被越来越广泛地应用于各种需要身份认证的领域；而通用生物证书是生物认证技术中的要素[2,3]。

通用生物证书(generic biometric certificate, GBC)是由权威机构(生物证书权威 BCA)颁发的绑定了用户身份及用户生物特征信息的并经过数字签名的数据结构[4]。

通用生物证书中生物特征模板存放生物证书主体

① 基金项目:国家自然科学基金项目(60873081)
收稿时间:2008-10-10

的生物特征信息，主要包括：版本号、生物特征模块、发行者及唯一标识、扩展信息、发行者签名、序列号、有效期、主体及其唯一标识等信息。该模板的安全关系到整个系统的安全和个人隐私。一旦生物特征信息泄漏，会造成系统不安全，同时也很可能造成个人在其他生物认证应用中受到安全威胁。因此，保证生物特征模板的安全至关重要。

鉴于 XML 自身具有的严密加密机制，同时 XML 的开发性、结构性、可移植性，其慢慢成为数据交换的标准格式；而生物证书也采用类似的保存格式，所以在此采用两者相结合的方式对信息进行存储加密传输是一种完全有效的安全方案。

4　XML

通常数据传输是使用基于 TCP 传输层的 SSL 安全方案。但是 SSL 只能对通信的全部信息加密，不能有选择的对 XML 中的部分数据进行加密。当需要传输大量数据但需要加密的数据却很少时，SSL 对全部数据加密导致传输速度很慢；当发送的数据需经过多方路由才能到达接收端时，因数据中的路由信息不能被加密，所以 SSL 加密就不再适用。

针对现有解决方案的局限和不足，在分布式数据交换中采用 XML 加密方案不失为一种有效的安全措施。

5　基于生物特征和XML的C/R认证方案

采用挑战/应答认证机制，虽然可以防止重放攻击，但不能防止假冒；同时为了弥补其在网络环境应用下的缺陷和单一的认证机制存在的各种不足以及生物特征信息在传输过程中的安全保密问题，本文将生物认证技术、XML 技术与 C/R 机制相结合，提出了一种基于生物特征和 XML 的 C/R 认证方案。

5.1 基于生物特征和 XML 的 C/R 认证的系统框架

(1)认证服务器

认证服务器主要包括信息处理模块、服务代理模块和认证服务器。信息处理模块主要完成对获取经过加密的用户信息进行解密，再传给认证服务器进行认证核对。服务代理模块主要完成截获用户发向资源服务器认证的请求连接,将其转发到认证服务模块进行用户的身份认证,它是实现客户端和认证服务模块认证连接转发的中间环节,当用户认证成功后为用户建立访问资源服务器的透明代理。使用服务代理模块的主要目的是实现用户信息数据库与认证服务器的分离,充分保证用户信息的安全。认证服务器主要完成与客户端的认证工作。各种用户的身份认证信息和本地的一些安全参数信息,都存放在用户信息数据库中。

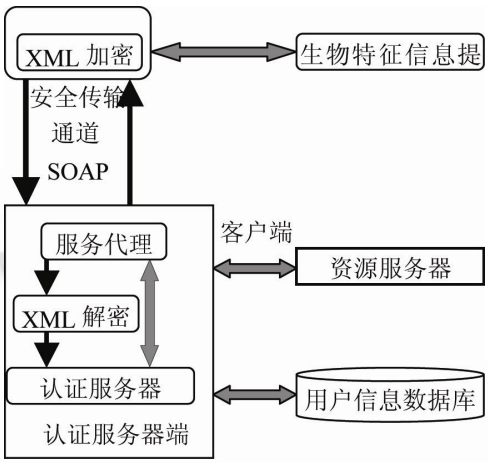

图 1　系统框架

(2)认证客户端

认证客户端位于内部网络和公共网络任何待认证的用户主机中。认证客户端主要实现系统和客户的管理,为终端用户提供一个简洁、方便的操作界面。同时获取用户的生物特征信息，并加密其信息，再向认证服务器发起请求。

5.2 认证流程

在用户入网认证之前首先在认证服务器端进行注册,这样用户成为网络资源服务器的合法用户。

在用户信息初始化完成之后,如果用户希望访问资源服务器的资源,必须首先通过认证服务器的认证。客户端与认证服务器之间需要完成如下四个消息的交互以完成两者之间的身份认证。

①(User,Ip)表示客户端发送给认证服务器待认证的特有用户名和机器 IP 号；

②Rand 表示认证服务器生成一个随机数 Rand,作为认证时的挑战；

③(UGBK,R)表示客户端发给服务器端的认证数据包；

④(Result)表示认证服务器发送给用户的认证结果。

具体认证过程如下：

(1)用户向服务器输入用户名或 ID 号发出认证请求，此用户信息经过 XML 加密机制加密后再传输给服务器；

(2)服务器解密获取用户信息，验证用户的合法性，只有通过系统的用户信息鉴别后才能进行下一步验证，若不是就拒绝提供服务。

(3)是合法用户，认证服务器产生一个随机挑战数 R，作为提问，发给客户端。

(4)客户端提醒用户输入用户生物特征信息。用户将自己的指纹、声音或其它生物特征信息记录下来，由系统自动提取用户的生物信息。系统对提取出的生物信息处理后，将其与挑战数 R 合并，并使用单向 hash 函数生成一个应答字符串。系统将所需生物信息组合成 XML 文档，再调用 XML 加密机制对其中的应答字符串进行加密，生成包含用户生物特性信息的 XGBK(XML 加密后的生物特征信息)，其中挑战数 R 就作为 XML 加密的密钥，最后将其封装成 SOAP 消息传送到服务器端。

(5)认证服务器将接受到的应答字符串，经过相应的处理再与自己的计算结果进行对比，若两者相同，则通过验证，若不相同则认证失败。

(6)认证服务器通知客户端认证结果。

由于传输过程的保密性，这就保证了此认证方案的可行性。验证过程如图 2 所示。

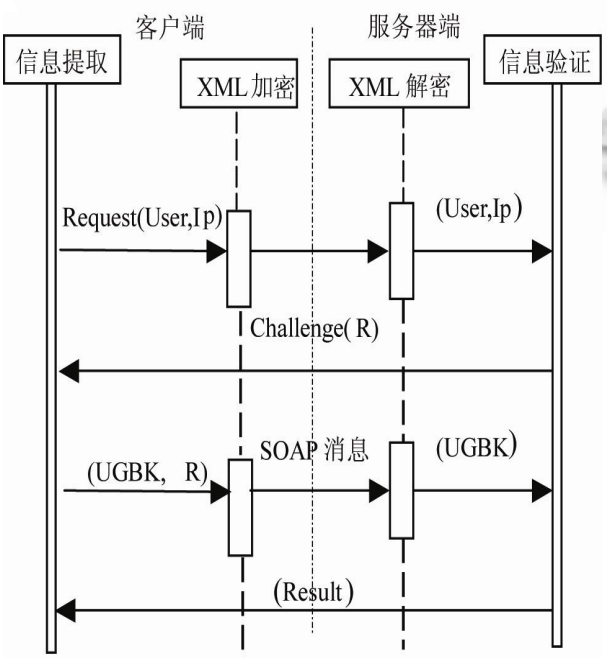

图 2　验证过程

5.3 XML 加、解密分析

5.3.1 XML 文档加密过程的实现

下面介绍了基于FrameWork2.0，采用C# 实现对 XML 数据进行加密解密的过程。在实现过程中使用 System.Security.Cryptography.Xml 命名空间中的类及 FrameWork2.0 中新增类 EncryptedXml 对 XML 文档中的元素进行加密。

(1)创建一个 XmlDocument 对象，利用它的 load 方法从磁盘装载要加密的 XML 文件。XmlDocument 对象包含要加密的 XML 元素。

(2)使用 RijndaelManaged 类创建一个新的会话密钥。创建 EncryptedXml 类的新实例，并用会话密钥对指定的元素进行加密。

(3)构造一个 EncryptedData 对象，然后用加密的 XML 元素的 URL 标识符填充它。URL 标识符使解密方知道 XML 包含一个加密元素。

(4)创建 EncryptedKey 对象，以包含加密的会话密钥。对会话密钥进行加密，将它添加到 EncryptedKey 对象中。

(5)创建一个新的 KeyInfo 对象，以指定 RSA 密钥的名称。将它添加到 EncryptedData 对象中。该元素用于帮助解密方识别解密时需要使用的非对称密钥。

(6) 最后将加密的元素数据添加到 EncryptedData 对象中。用 EncryptedData 元素替换原始 XmlDocument 对象中的元素。保存 XmlDocument 对象。

5.3.2 XML 文档解密过程的实现

若要对 XML 元素进行解密，接收方用私钥对会话密钥进行解密，然后使用会话密钥对文档进行解密。

(1)加载加密文档

```
XmlDocument xmlDoc = new XmlDocument();
xmlDoc.PreserveWhitespace=true;
xmlDoc.Load(".xml");
```

(2)添加密钥/名称映射，以将 RSA 密钥与要解密的文档中的元素关联起来。

```
EncryptedXml exml = new EncryptedXml(Doc);
exml.AddKeyNameMapping(KeyName, Alg).
```

(3)调用 DecryptDocument()方法对<EncryptedData>元素进行解密。此方法使用 RSA 密钥对会话密钥进行解密，然后自动使用该会话密钥对 XML 文档进行解密。它还用原始纯文本自动替换

<EncryptedData> 元素。并保存 XML 文档。

6 实验结果及安全性分析

6.1 实验结果分析

为了验证本方案的可行性和可操作性，本文使用 FVC2002 DB2 指纹库作实验测试库，对此方案进行测试。实验结果见图 3。FVC2002 DB2 中的 800 幅指纹图像，分为 10 组，其中每组 8 枚指纹。在对 800 幅指纹图像进行测试后，实验结果为，在此方案中进行指纹处理和比对的速度为 350 枚/秒，误匹配率 FMR100 是 8.041%，误匹配率 FMR1000 是 14.058%。实验结果表明，在此方案内由于生物信息提取终端的处理能力较低，同时要实现特征信息转换加密处理和匹配，造成识别准确度不是特别高，数据转换加密速度较慢。这是将来需要对特征提取终端继续研究改进的方向。

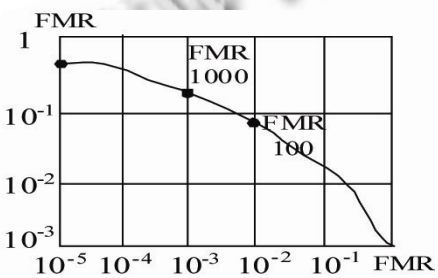

图 3 方案实验结果

6.2 安全性分析

和现有的 C/R 认证系统相比，基于生物特征和 XML 的 C/R 认证系统在实施应用方面更为通用和方便。具有以下特点:

(1)用户信息传输的保密性

身份认证系统中的所有重要数据,如密钥、口令等,均是以密文形式存储、传输；同时整体信息在传输过程中都以加密后的 XML 文档和 SOAP 消息的方式进行传输，更加保证了信息的安全。

(2)防止重放攻击

由于采用了挑战/应答认证机制,使得每次认证时认证服务器均会向客户端发送一个唯一的随机数，不会重复。因此,如果黑客截获了某一次的签名信息试图重放，则不会认证成功；如果截获了服务器发向客户端的随机数，由于没有私钥，也不可能正确签名，所以也不会认证成功。

(3)使用更便捷

在进行数据签名操作时,只需提取签名人的生物特征信息便可重构其签名私钥信息以完成签名操作。该方案避免了在绝大多数安全应用系统中,用户私钥必须存放于硬件设备(如智能 IC 卡或智能 key) 中的限制。不必担心硬件设备丢失、损坏所带来的损失。

(4)系统只允许单进程访问

密钥算法可以采用比较流行的 MD5 算法，也可以使用相对来说更加安全的 SHA-1 和 IPEMD-160。这样，算法、密钥、运算三个因素都是安全的，也就确保了整个认证过程的安全。

(5)安全性更高

本文充分利用了生物证书认证可以防止用户名和口令被窃取、抗抵赖，挑战/应答认证方式可以有效防止重放攻击的优势，把两者结合起来,使其相互补充、相辅相成；同时结合 XML 自身具有的严密安全机制，从而可为用户提供更强的身份认证功能。

7 总结

本文将生物认证技术、XML 技术与挑战/应答身份认证机制相结合，提出了一种全新的身份认证机制，克服了传统的单一认证机制存在的不足，通过用户私钥和生物特征信息两个因素来实现用户的身份认证，同时又引入了 XML 加密技术，从而达到了较高的安全性，对身份认证技术的研究具有一定的参考价值。

参考文献

1 王小妮,杨根兴.基于挑战/应答方式的身份认证系统的研究.北京机械工业学院学报, 2003,4:45-61.

2 Jain AK, Bolle R, Pankanti S. Biometrics: Personal Identification in Networked Society.Norwell,MA: Kluwer, 1999.

3 Wayman JL. Fundamentals of Biometric Authentica-tion Technologies. Int. J. Image Graph, 2001,1(1):93－113.

4 李涛,欧宗瑛.基于个人特征的身份认证技术的发展与运用.计算机工程, 2000,12:62-84.

5 Chris Knowles，Stephen Mohr.Professional ASP.NET XML With C#.Wrox Press Ltd, Inc 2002,12:128-134.

6 禹勇. XML 安全的研究与应用.西安交通大学, 2005(29).