基于联机手写签名和数字证书融合的 Web Service 身份认证研究*)

袁永峰 李 彬 王宽全

(哈尔滨工业大学 计算机科学与技术学院 哈尔滨150001)

摘 要 手写签名是个人独有的生物行为特征,可以用来鉴别个人身份。本文提出一种基于联机手写签名和数字证书融合的 Web Service 身份认证方案,该方案把数字证书和所有者的生物特征相结合,有效地解决了验证数字证书的使用者和所有者是否是同一实体的问题。本文采用 SOAP 协议用 XML 数字签名和加密技术封装用户和服务器之间的通信消息,为 Web Service 的信息交换提供可靠保障。

关键词 联机手写签名,数字证书,Web 服务,简单对象访问协议

An Authentication for Web Service Based on On-Line Handwritten Signature and Digital Certificate

YUAN Yong-Feng LI Bin WANG Kuan-Quan

(The School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001)

Abstract Handwritten signature is unique behavioral biometric characteristic of human and can be used to identify users. This paper proposes a novel authentication scheme about Web Service that combines the digital certification with on-line handwritten-signatures, which provides a good solution to bind digital certificate with its owner by his biometrics. The information between the user and the server is encapsulated into SOAP messages with both XML digital signature and XML encryption and the transaction can be conducted securely on Web service.

Keywords On-line handwritten-signature, Digital certificate, Web service, SOAP

1 引言

Web Service 是指由企业发布的、完成其特别业务需求的应用服务,其他企业或组织可以通过 Internet 来动态访问并使用这些在线服务[1]。Web Service 采用 SOAP、WSDL、UDDI 等标准的 XML 协议及相关技术,统一地封装信息、行为、数据表现以及商务流程,无需考虑其应用的编程语言和运行环境。因此,Web Service 技术受到广泛关注,IBM、Microsoft 和 SUN 等 IT 业大公司纷纷介入,制定他们的 Web Service 战略——IBM 的 Websphere, Microsoft 的 .Net 以及 SUN 的 SUN ONE 平台。可以预见 Web Service 将成为未来的电子商务、电子政务等网络应用的发展方向。

由于 Internet 的开放性,潜在着信息被干扰、窃取和篡改的风险。如何保证 Web service 的可靠性和安全性问题,深受人们的关注。手写签名是人的一种特有的行为特征,作为身份鉴别的一种有效手段,一直被人们广泛接受并具有法律效力。例如工作或会议签到、收信人确认签名、银行开户或提款签名、文件合同的签署等等。随着科技的发展,基于联机手写签名的身份鉴别技术越来越受到人们的关注,并取得了很大的发展。本文把联机手写签名技术和现有的数字签名技术相结合,提出一种基于 SOAP 协议的身份认证方案。这个方案,不仅很好地解决 Web Service 的安全问题;同时,也充分发挥 Web Service 无障碍的技术优势。

2 SOAP 协议和 XML 数字签名技术

2.1 SOAP 协议

简单对象访问协议 SOAP(Simple Object Access Protocol)[3]是一种在分布式环境中交换结构化信息的轻型协议。它利用 XML 技术定义了一个消息框架机制,该机制可以通过多种的传输协议(如 HTTP、FTP、SMTP 等)在客户端和服务器端传输命令和参数,而无需考虑编程语言、对象模型、操作系统、硬件平台等具体的应用环境。因为 SOAP 是一种轻型协议,所以其消息框架机制没有直接提供保障 SOAP 的内容可靠的安全机制,但是可以利用 SOAP 安全扩展[4]来实现。通过 SOAP 标题元素与安全扩展相结合,把安全元素添加到 SOAP 消息中,以此保护 SOAP 内容的机密性和完整性。

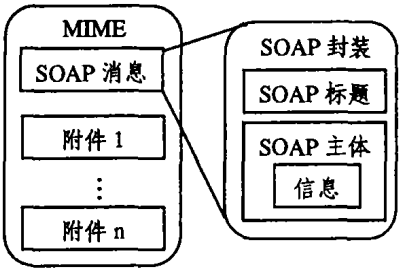

图1 SOAP 结构图

2.2 XML 签名和加密

XML 签名[5]利用现有的数字签名技术对整个 XML 文档或者 XML 文档的特定部分的任何类型的数字内容进行签署,以 XML 的格式表示该数字签名的元素,并将该数字签名结合到该文档中,从而保证数据的完整性。

XML 加密[6]同 XML 签名类似,它构建在现有的加密算法基础上,为加密和解密整个 XML 文档或者 XML 文档的特

*)基金项目:哈尔滨市科技攻关项目(2003AA1CG055-10)。袁永峰 硕士研究生,主要研究方向为手写签名认证和信息隐藏;李 彬 博士研究生,主要研究方向为模式识别、信号处理和手写签名认证;王宽全 教授,博士生导师,主要研究方向为计算机网络、模式识别和图像处理。

定部分的任何类型的数字内容，提供一个标准的表示格式和处理模型。利用 XML 加密技术可以保证数据的机密性和可靠性。

3 Web Service 的安全性

3.1 Web Service 的主要安全要素

在实现任何 Web 服务时都应当考虑以下五个主要安全要素[2]：

(1) *机密性* 必须保证用户参与的 Web 事务中，他们的敏感数据是安全的，只能被那些经授权的个人查看。不会被泄漏给未授权的个人。

(2) *身份验证* 对访问 Web 服务的实体提供的标识信息进行验证，使数据的接受方能够确定数据的发送方的身份，进而确认该实体是否有权获得服务。验证通过后，该实体就被称为用户，可以获得服务；否则，拒绝该实体的服务请求。

(3) *完整性* 必须确保用户和服务之间交换的信息是真实、有效、及时并且未加任何改动的。为了保证数据的完整性，数据接收方能够检测出未经授权的数据修改。

(4) *非否认性* 必须防止信息的发送方否认先前已执行的动作或否认发送数据内容。

(5) *授权* 必须限制用户的查看和操作权限，防止他们利用系统的安全漏洞，越权查看或者操作某些特定的、机密的信息。

3.2 Web Service 的身份认证

目前，Web 服务的身份认证形式有如下几种：

(1) HTTP *基本身份认证* 这是一种基于用户名(或者 ID)和口令的验证方式。用户名以明文发送，密码以 Base64编码的方式传送。HTTP 基本身份认证是目前最常见的方式，也是最简单的验证方式。但是这种方法很不安全，Base64编码非常容易破解。

(2) *基于 HTTP Forms 的身份认证* 用户提供的用户名和口令以 HTTP 表单形式发送给 Web 服务端验证身份。这种身份认证方式也是一种非常薄弱的认证方式。

(3) *基于数字摘要的身份认证* 这里通过 Hash 算法和加密算法，把口令以加密的数字摘要形式传送。在服务端，把收到的数字摘要同预先得到的数字摘要进行匹配，以验证身份。数字摘要形式比前面两种方式安全，但也是有限的。它仅仅提供身份认证，并不能保证数据传输的完整性、非否认性。

(4) *基于数字证书的身份认证* 这种方法通常和传输层 SSL 协议配合使用。它要求用户和服务提供者从可信赖的 CA (Certification Authority) 获得标准的数字证书(如 X.509)。Web 服务提供者首先验证用户的证书是否有效，验证通过后，双方交换密钥，通过 SSL 协议建立安全通道。在理想的情况下，由于有 CA 证书的存在，这种方式是安全和可信的。但在实际情况中，无法保证证书的使用者和证书的所有者是同一实体。

(5) *基于 XML 扩展的身份认证* 这是一种新兴的安全方案。它扩展了现有的 XML 文档模式，结合数字签名技术为 XML 文档添加了安全构件，并且为 Key 管理和分发设定一套完整的规范和标记语言(如 XKMS、XKISS、XACML、SAML 等)。但是 XML 扩展的身份认证仍然依赖于数字证书，也存在(4)中的出现的问题。

综上，前三种认证方式安全性较低，不满足建立安全、可靠的 Web Service 的需要；后两种方式由于使用了数字证书，相对安全性较高。使用数字证书，不仅可以有效地验证身份和授权，而且利用证书中约定的密钥机制，可以保证传输数据的机密性和完整性。但是，它不能充分满足非否认性。因为这两种身份认证的安全是建立在私钥安全和数字证书可靠的假设基础之上，认为用户和 Web 服务的数字证书提供的标识是不可破坏的，证书的所有者也是证书的使用者，只有证书的所有者才有证书验证的私钥。然而，在现实生活中，数字证书的使用只是证明使用了某个特殊标识，它并不能证明该标识使用者就是该标识的真正所有者。所以，数字证书本身不带有所有者信息，不能满足非否认性。

3.3 联机手写签名与数字证书相结合

人们的书写过程受到大脑神经(心理)和身体器官(肌肉和关节)控制，是一种长期训练形成的定型条件反射。签名行为反映了人的身体机能长期形成的书写习惯，具有很强的个体性，这种个体性不易伪造，可以充分用于鉴别身份。联机手写签名，通过数位板实时采集个体的书写信号，不仅记录笔迹的静态特征(笔尖运动的空间位置信息)，而且记录书写的压力、速度、加速度等动态特征。这些特征不仅提供了丰富个性化的信息，也为人的身份鉴别提供可靠依据。本文采用基于结合动、静态特征的一维曲线弹性匹配的联机手写签名鉴别算法[8]，该算法在实验过程中体现出较好的鉴别性能和精度。对110人的1100个真实样本和440个经过一定训练的伪造样本进行测试，其中对于每个签名者，5个真实签名作为参考样本，另外5个真实签名和4个伪造签名用来测试。我们得到的错误拒识率(FRR)为1.8%，错误接受率(FAR)为2.5%。

把联机手写签名验证和数字证书相结合。在认证用户身份时，同时验证数字证书和该证书使用者的联机手写签名，利用使用者的联机手写签名来确认该证书的所有者和使用者是否是同一实体；另一方面，利用数字证书中约定的密钥机制加密联机手写签名，保证联机手写签名在传输过程中的安全。认证方案如下：

初始约定：认证中心(C)颁发合法的数字证书给用户(U)和 Web 提供者(WS)，并且注册用户的联机手写签名(F)。

请求身份验证：

(1) 用户输入联机手写签名(F')；

(2) 对联机手写签名(F')使用 hash 函数得到 hash 值 $sig(F')$；

(3) 用认证中心的公钥加密(F')和 $sig(F')$得到 $E_c(F', sig(F'))$；

(4) 最后用 Web 提供者的公钥加密 $E_c(F', sig(F'))$和用户的数字证书 $Cert_U$，并发送认证消息 $E_{ws}(E_C(F', sig(F')), Cert_U)$。

身份认证：

(1) Web 提供者用自己的私钥解密认证消息 $E_{ws}(E_c(F', sig(F')), Cert_U)$得到 $E_C(F', sig(F'))$和 $Cert_U$；

(2) 用认证中心的公钥 E_C 加密，$E_C(F', sig(F')), Cert_U$ 和 $Cert_{ws}$，得到 $E_C(E_C(F', sig(F')), Cert_U, Cert_{ws})$，然后转发给认证中心认证；

(3) 认证中心用自己的私钥解密得到(F')、$sig(F')$、$Cert_U$ 和 $Cert_{ws}$；

(4) 验证 Web 服务提供者数字证书 $Cert_{ws}$；

(5) 验证(F')的完整性，对(F')做 hash，是否等于 $sig(F')$，如果不等于，产生出错信息跳到第5步，否则继续；

(6) 验证联机手写签名(F')和数字证书 $Cert_U$；

(7) 如果验证成功,向 Web 提供者返回确认信息,否则,返回出错信息。

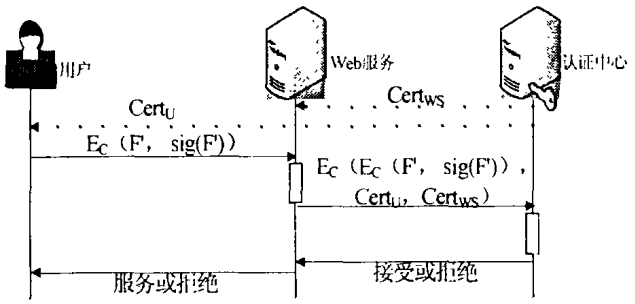

图2 认证方案

综上,联机手写签名验证和数字证书验证的结合,从真正意义上实现数字证书的非否认性,充分满足了 Web Service 的五个主要安全要素,为 Web 服务提供一个可信赖的安全保证。

4 身份验证方案实现

4.1 Web 服务认证框架

Web 服务认证框架由用户、Web 服务提供者和认证中心三方面构成(如图3)。这里认证中心是可信赖的颁发数字证书的权威机构。Web 服务提供者和认证中心建立专用、安全的通道。Web 服务提供者把用户身份注册和身份认证授权给认证中心,并且信任认证中心的验证结果。

认证过程如下:

(1)用户向 Web 服务提供者发出服务请求;

(2)Web 服务把用户的请求重新定向到认证中心;

(3)认证中心向用户发出身份认证质询;

(4)用户向认证中心提供合法的凭证;

(5)如果认证中心验证通过,通知 Web 服务该用户验证通过,并且把用户的凭证转发给 Web 服务;否则,并通知 Web 服务该用户非法;

(6)Web 服务根据认证中心验证结果,响应用户请求,决定提供服务还是拒绝服务;

(7) 当用户退出服务或者长时间没有事务活动时,Web 服务提供者撤销连接,并通知认证中心。认证中心记录此次认证,并取消此次认证合法性。

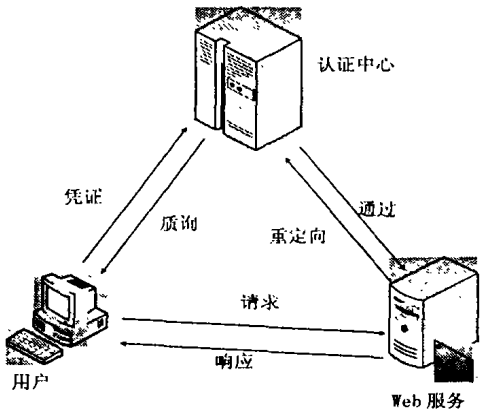

图3 Web 服务示意图

4.2 身份注册[7]

用户向 Web 服务发出请求,Web 服务根据用户请求内容做出响应。如果用户没有注册,则把用户的请求重新定向到认证中心,由认证中心提供 Web 用户注册和认证的服务。

认证中心按 XML 密钥管理规范(XMKS)和 XML 密钥注册服务规范(XKRSS),注册用户。认证中心按事先和 Web 服务提供者约定的规则,让客户提供相关信息。其次,用户注册联机手写签名,并测试联机手写签名注册结果;如果测试失败,重新注册。再次,为用户生成数字证书,按用户约定安全的通信方式,向其颁发数字证书。最后,认证中心为该用户建立注册档案。

4.3 身份验证

认证中心向用户发送一个质询和认证中心的凭证信息(数字证书),用户端验证凭证信息确定是否是认证中心发出。如果证书验证通过,用户提供必要的信息,并输入联机手写签名;在用户端自动提取联机手写签名的行为特征(包括静态特征和动态特征)。最后,用户数字证书转换 XML 元素(ds:X509Data),提取出来的联机手写签名特征用认证中心的公钥加密,生成 XML 元素(enc:EncryptedData),把这些元素封装到 SOAP 消息中(如表1),向认证中心发出认证请求。

表1 封装验证请求的 SOAP 消息

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP-ENV:Envelope …>
  <SOAP-ENV:Header>
    <ID id="identity">209731</ID>
    <username id="username">Linda</username>
    <SOAP-SEC:Encryption …>
      <SOAP-SEC:Reference
        id="#handSignature"/>
      </ SOAP-SEC:Encryption >
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <ValidateRequest …>
    … …
    <QueryKeyBinding>
    … …
    <ds:X509Data>
      <ds:X509Certificate>
        MIICAjCCAgAwIBIQlzQovIE …
      </ds:X509Certificate>
    </ds:X509Data>
    … …
    </QueryKeyBinding>
  </ValidateRequest>
  <enc:EncryptedData … … id="handSignature">
    <ds:KeyInfo …>
      <ds:KeyName>cn96epgc</ds:KeyName>
    </ds:KeyInfo>
    <CipherData>
      <CipherValue>
        MII3LMmeohNYfCXTHL… … …
      </CipherValue>
    </CipherData>
  </enc:EncryptedData>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

认证中心解密用户端加密的数据,同时验证用户的数字证书和联机手写签名,确认该证书的使用者和所有者是否是同一实体。如果用户身份验证通过,认证中心为这次验证创建唯一的标识。认证中心用自己的数字证书,对唯一的标识、用户的联机手写签名、数字证书和时间戳信息作数字签名;用用户的公钥把数字签名和 Web 服务提供者的公钥加密发给用户,把数字签名和用户的公钥用 Web 服务提供者的公钥加密和验证通过消息一同发给 Web 服务提供者(如表2)。至此完成验证,并为用户和 Web 服务提供者建立可靠连接。

表2 封装验证响应的 SOAP 消息

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP-ENV:Envelope …>
<SOAP-ENV:Header>
  <SOAP-SEC:Signature …>
    … …
    <ds:SignatureMethod Algorithm=…/>
    <ds:Reference
```

```
        URI="http://Reg-biometrics.hit.edu.cn/xkms/21438">
        <ds:DigestMethod Algorithm=…/>
        <ds:DigestValue>
          j6lwx3rvEPO0vKtMup4NbeVu8nk=
        </ds:DigestValue>
      </ds:Reference>
        … …
      <ds:SignatureValue>
        MC0CFFrVLtRlk=
      </ds:SignatureValue>
        … …
    </SOAP-SEC:Signature>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <ValidateResult …>
      <KeyBinding Id="xxxxxx">
        … … …
        <ds:RSAKeyValue>
          <ds:Modulus>zvbTd…</ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
        </ds:RSAKeyValue>
        … …
      </KeyBinding>
    </ValidateResult>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

当用户退出服务或者长时间没有事务活动时，Web 服务提供者停止服务，撤销连接，并通知认证中心，认证中心记录，并取消此次认证的合法性。

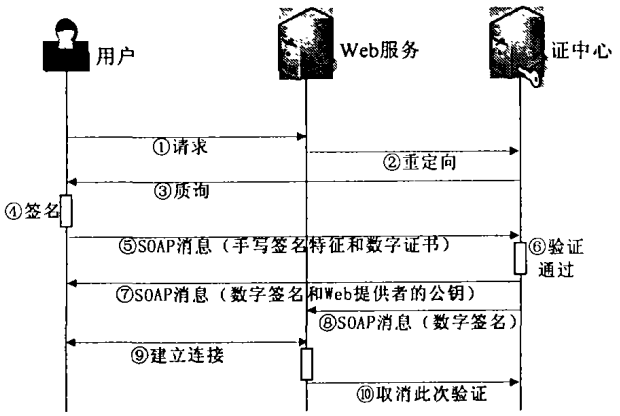

图4 合法用户的认证事件流

结束语 本文把联机手写签名和数字证书相结合进行身份认证。利用联机手写签名的生物特征，准确地鉴别并标识个人身份，保证了证书的所有者和使用者是同一实体；另一方面，利用数字证书中约定的密钥机制加密联机手写签名和传输数据，从而保证了该数字证书签署的数字签名的可靠性和非否认性，为 Web Service 提供了可靠的身份认证机制。同时，由于采用 SOAP 协议来交换信息，充分发挥 Web Service 支持多协议、跨平台无障碍的优势，提供了更广泛的身份认证服务。

参 考 文 献

1 吴应良. 基于 Web Service 的动态电子商务体系结构. 计算机应用研究，2003(7)：20～23

2 Nakamur Y, Hada S, RyoMeyama. Towards the Integration of Web Service Security on Enterprise Environment. In: Proc. of the 2002 Symposium on Applications and the Internet (SAINT '02w), 2002. 166～175

3 Simple Object Access Protocol (SOAP) 1. 1. http://www. w3. org/TR/SOAP/. 2000, 5

4 SOAP Security Extensions: Digital Signature. http://www. w3. org/TR/SOAP-dsig/. 2001

5 XML-Signature Syntax and Processing. http://www. w3. org/TR/xmldsig-core/. 2000

6 XML Encryption Syntax and Processing. http://www. w3. org/TR/xmlenc-core/. 2002

7 XML Key Management Specification 2. 0. http://www. w3. org/TR/xkms2/. 2003

8 Li Bin, Wang Kuanquan, Zhang David. On-Line Signature Verification for E-Finance and E-Commerce Security. The In: Second Intl. Conf. on Machine Learning and Cybernetics (ICMLC2003). Nov. 2003. 3002～3007

（上接第121页）

标准输出(d)

0.8	0.9	0.7	0.4	0	−0.4	−0.8	−0.9	−0.8
0.9	1.0	0.8	0.5	0	−0.4	−0.8	−1.0	−0.9
0.8	0.8	0.7	0.4	0	−0.4	−0.7	−0.8	−0.8
0.4	0.5	0.4	0.2	0	−0.2	−0.4	−0.5	−0.4
0	0	0	0	0	0	0	0	0
−0.4	−0.5	−0.4	−0.2	0	0.2	0.4	0.5	0.4
−0.7	−0.8	−0.7	−0.4	0	0.4	0.7	0.8	0.8
−0.9	−1.0	−0.8	−0.5	0	0.4	0.8	1.0	0.9
−0.8	−0.9	−0.7	−0.4	0	0.4	0.7	0.9	0.8

网络运行3440次后，平均误差为0.075130，最大误差为0.153548，连接权实验结果如下：

权(W)

−6.639129	0.039305	0.782633	0.345540	2.040181
−0.250256	−0.462557	−0.393224	−0.513422	0.408255
0.097718	−0.030444	1.190157	−1.277041	−0.106535
0.871643	−0.264692			

实验系统界面以及误差曲线见附图(略)。

参 考 文 献

1 Zhang Qinghua, Benveniste A. Wavelet networks. IEEE Trans. on Neural Networks, 1992, 3(6): 889～898

2 Zhang Jun, et al. Wavelet neural networks for function learning. IEEE Trans. On Neural Networks, 1995, 43(6): 1485～1497

3 Ladde G S, Lakshmikantham V, Vatsala A S. Monotone iterative techniques for nonlinear differential equations. New York: Pitman, 1985

4 Heikkila S, Lakshmikantham V. Monotone iterative techniques for discontinuous nonlinear differential equations. New York: Marcel Dekker Inc., 1994

5 Guo Dajun, Lakshmikantham V. Nonlinear problems in abstract cones. New York: Academic Press, 1988

6 Guo D, Sun Jingxian. Nonlinear Integral Equations. Jinan: Shandong Science and Technology Press, 1987

7 Pao Y H, et al. Neural-net computing and intelligent control systems. Int. J. Control, 1992, 56: 263～289

8 张苗生，刘贵忠，刘峰. 一种自适应小波网络的构造及学习算法. 中国科学(E辑)，2001，31(2)：172～181

9 吕立华，宋执环，李平. 一种小波网络设计新方法. 信息与控制，2002，31(1)：14～18

10 陈哲，冯天瑾. 小波分析与神经网络结合的研究进展. 电子科学学刊，2000，22(3)：496～504

11 Pahl G, Beitz W. Engineering Design. London: Design Council, 1984