文章编号:1001 - 9081(2007)02 - 0318 - 03

网络采购系统中安全机制的研究与实现

张 璐,张 璟,井 浩,李军怀
(西安理工大学 计算机科学与工程学院,陕西 西安 710048)
(olivia0318@vip.sina.com)

摘 要:针对网络采购系统中的安全问题,提出了一种网络采购系统安全机制模型,综合应用数字证书与 ASP.NET 的 Forms 身份验证相结合的认证技术,以及数据加密和数字签名技术,实现了其安全机制。同时,基于 B/S 模式下实现加密与数字签名的问题,开发了电子合同加密和数字签名智能客户端程序,为构造安全实用的大型网络采购系统奠定了技术基础。

关键词:网络采购;安全机制模型;身份认证;加密;数字签名
中图分类号: TP393.08 **文献标识码**:A

Research and implementation of security mechanism in electronic procurement system

ZHANG Lu, ZHANG Jing, JING Hao, LI Jun-huai
(*College of Computer Science and Engineering, Xi' an University of Technology, Xi' an Shaanxi* 710048, *China*)

Abstract: This paper intended to solve the security problem of electronic procurement system. A model of security mechanism was put forward with the help of comprehensive application of the authentication technique combined with digital certificate and ASP.Net's forms authentication, and of the data encryption technique and the digital signature technique. At the same time, concerning the problems of implementation of encryption and digital signature in B/S mode, this paper developed the electronic contract encryption and digital signature smart client program, and prepared the technical ground for the construction of secure, practical, and big electronic procurement system.

Key words: electronic procurement; security mechanism model; authentication; encryption; digital signature

随着我国电子商务的日益成熟以及信息技术的不断发展,促使电子商务在企业中的应用逐步从单一的信息发布向更高层次的整合应用发展,从而推动了企业采购由传统模式向网络采购的转变。网络采购是一个基于 Web 体系的企业采购解决方案,其安全机制的核心是客户端与服务器之间的相互认证、安全通信,以及传输信息的机密性、完整性和不可否认性。

1 客户端与服务器认证

传统的网络认证模式无法确保客户端与服务器之间的相互认证以及安全通信。为了避免攻击者冒名申请采购单和审批采购单必须要实现服务器对客户身份的认证,同时为了防止攻击者恶意破坏,客户端也需要对服务器进行认证并且实现安全通信。

1.1 信息的机密性、完整性以及不可否认性

我们已经开发的网络采购系统网上洽谈模块为企业和客户提供了网上会谈的平台。在会谈过程中需要通过网络多次传输电子合同,因此必须着重考虑洽谈双方身份的真实性以及传输合同的有效性。合同的有效性包括其在传输过程中不被伪造、篡改,即合同的机密性、完整性,以及确认合同发送者的真实身份,即合同修改者或者签署者身份的不可否认性。

1.2 B/S 模式下实现加密与数字签名的问题

微软.NET 的 CAPICOM 组件封装了加密体系模型(CryptAPI)的一些复杂操作,利用 ActiveX 和 COM 对象进行加密和数字签名,能够实现 B/S 模式客户端加密和数字签名。很多应用系统在实现 Web 系统加密及数字签名时都选择 CAPICOM 组件,依靠它能方便地获取客户数字证书及其私钥的特性。但是利用 CAPICOM 组件开发存在一些弊端:首先,客户需要手动注册 CAPICOM.DLL,这为系统的部署带来诸多不便;其次,在 Web 系统中应用 CAPICOM 一般采用 JavaScript 脚本技术,而 JavaScript 不能访问客户端本地的文件系统,不符合系统获取待签名电子合同文件的要求;再次,CAPICOM 的实施需要在客户端下载安装 ActiveX 控件,而其本身存在着安全隐患。

为了解决上述问题,本文提出了网络采购系统中的安全机制模型及其软件结构,综合应用数字证书与 ASP.NET 的 Forms 身份验证相结合的认证技术,以及加密和数字签名技术,开发电子合同的加密和数字签名智能客户端程序,实现了客户端与服务器之间的相互认证,确保了传输信息的机密性、完整性以及不可否认性。

收稿日期:2006 - 08 - 28;**修订日期**:2006 - 10 - 23 **基金项目**:陕西省科学技术研究发展计划项目支持(2006K04-G10)

作者简介:张璐(1981 -),女,陕西西安人,硕士研究生,主要研究方向:计算机网络、分布式系统应用、Web 应用系统开发; 张璟(1952 -),男,陕西宝鸡人,教授,博士生导师,主要研究方向:计算机网络、分布式系统应用、Web 应用系统开发; 井浩(1972 -),男,陕西西安人,博士研究生,主要研究方向:制造网格、网格技术在企业信息化集成中的应用; 李军怀(1969 -),男,陕西宝鸡人,副教授,主要研究方向:分布式计算.

2　网络采购系统中安全机制模型及其软件结构

2.1　网络采购系统中安全机制模型

定义 1　网络采购系统安全机制(Electronic Procurement Security Mechanism,EPSM)可定义为一个三元组:

EPSM = (A,Sc,St)

其中 A:用户身份认证(Authentication);

Sc:客户端与服务器之间安全通信(Secure Communication);

St:电子合同安全传输(Secure Transmission)。

定义 2　用户身份认证可定义为如下二元组:

A = (Fa,Cv)

其中 Fa:Forms 身份验证(Forms Authentication);

Cv:数字证书验证(Certificate Validate)。

定义 3　客户端与服务器之间安全通信可定义为如下二元组:

Sc = (Sa,Ca)

其中 Sa:服务器身份验证(Server Authentication);

Ca:客户端身份验证(Client Authentication)。

定义 4　电子合同安全传输可定义为如下二元组:

St = (E,Ds)

其中 E:电子合同加密(Encryption);

Ds:电子合同数字签名(Digital Signature)。

2.2　网络采购系统中安全机制的逻辑结构

根据安全机制模型可得到网络采购系统中安全机制软件模块结构,如图 1 所示。

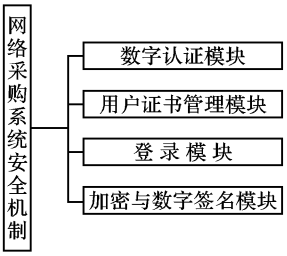

图 1　网络采购系统中安全机制逻辑结构

1)数字认证模块

本模块支持用户数字证书的申请、下载、安装以及管理。用户数字证书一般由受信任的第三方机构颁发。根据用户需求,同时考虑到网络采购系统中安全机制设计方案的完整性,采用自建企业级证书颁发机构的方案,构建基于 Windows Server 2003 的数字认证模块。证书的管理在服务器上维护,主要完成证书的审核颁发、吊销等工作。

2)用户证书管理模块

本模块支持用户申请吊销数字证书以及管理员获取吊销申请信息。为了避免冒名申请或者对非有效数字证书进行吊销,要求用户必须通过身份认证才能提出申请。管理员获取申请吊销的用户信息,并在服务器上进行证书吊销以及失效证书列表发布工作。

3)登录模块

本模块应用客户端数字证书与 ASP. NET 的 Forms 身份验证相结合的认证技术,完成用户身份认证功能。网络采购系统资源存在两个受保护级别:一是初级保护级别,通过 Forms 身份验证便可访问;另一个是高级保护级别,用户不仅要通过上述验证,而且系统要对客户端数字证书进行识别,通过认证后方可允许访问。系统程序根据用户选择的不同模块进行相应的身份认证。

4)加密与数字签名模块

本模块支持电子合同查看、加密和数字签名功能。允许用户在客户端获取洽谈合同并进行核对,若是企业洽谈员将从服务器端获取电子合同,若是商业用户将从本地文件系统中获取合同。用户完成洽谈合同核对工作后将进行合同的加密以及数字签名。

3　网络采购系统中安全机制的实现

3.1　客户端身份认证方案与实现

本系统采用 ASP. NET 的 Forms 身份验证与客户端数字证书相结合的双重认证方案。

方案设计:当用户访问受限资源时必须提供用户名和密码,系统程序通过查询数据库对其进行验证,确认该用户名与密码的有效性。如果有效,获取该用户数字证书中客户信息与登录信息进行比较,结果一致就允许访问高级保护级别的资源,否则仅允许访问初级保护级别资源。如果用户名与密码无效,拒绝访问。

方案实现:客户数字证书字段由. NET Framework 中的 HttpClientCertificate 类提供。自定义 Check( ) 函数,利用 HttpClientCertificate 类获取数字证书的 Subject 域,提取字段列表中的 CN 值与登录信息比较,并且根据比较结果决定是否响应用户的请求。这种双重认证方案使系统能够对资源根据其受保护级别区别处理,对于高级别的保护资源而言,访问者必须既是系统的有效用户同时也具有数字证书,并且该证书与用户之间具有关联。

3.2　加密/数字签名与解密/数字签名验证的实现

3.2.1　*加密/数字签名实现原理*

为了保证电子合同的机密性,我们使用对称加密算法加密合同,同时为了保证对称加密算法的有效实施,使用接收者数字证书中的公钥加密对称算法中的会话密钥以及初始化向量,与密文一同形成数字信封。为了保证电子合同的完整性并且提高实施数字签名的速度,对合同进行散列运算,形成数字摘要。为了保证电子合同的不可否认性,对合同的数字摘要实施数字签名。加密与数字签名实现原理如图 2 所示。

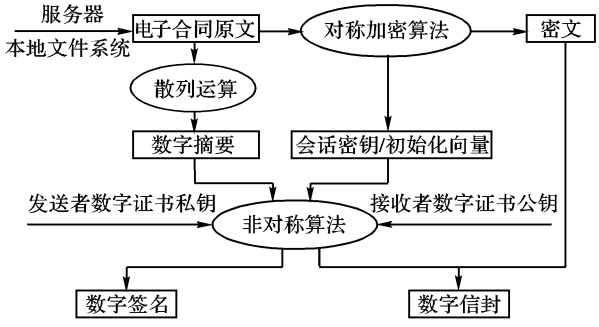

图 2　加密/数字签名实现原理

3.2.2　*解密/数字签名验证实现原理*

接收者使用自己数字证书中的私钥对加密的会话密钥以及初始化向量进行解密,然后使用解密得到的会话密钥和初始化向量解密电子合同密文,解密过程的成功实施确保了合同的机密性。接收者使用发送者数字证书中的公钥对数字签名进行验证,得到数字摘要,验证过程的成功实施确保了合同的不可否认性。使用同样的散列算法对解密得到的合同进行

运算得到新的数字摘要,将它与接收到的数字摘要进行比较,如果一致确保了合同的完整性。解密与数字签名验证实现原理如图 3 所示。

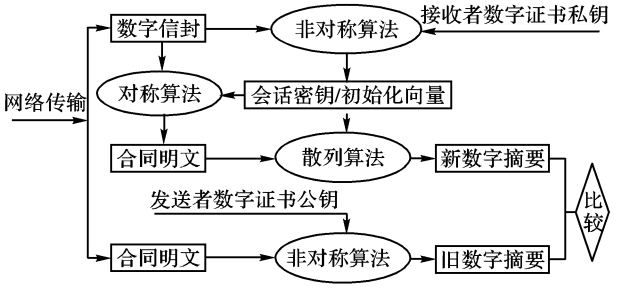

图 3 解密/数字签名验证实现原理

3.2.3 加密/数字签名与解密/数字签名验证算法实现

System. Security. Cryptography 命名空间支持 Rijndael 对称算法和 RSA 非对称算法。Rijndael 算法适合大信息量的数据加密,而 RSA 算法既能进行数据加密也可以进行数字签名,适用于网络中传输数据的加密和身份鉴别。因此,选择这两种算法结合洽谈双方的数字证书来实施电子合同的加密与数字签名。同时,. NET Framework 2. 0 新增 X509Certificate2 类表示 X. 509 证书,选择该类对客户端本地证书存储区中数字证书进行操作。

加密首先要生成随机会话密钥以及初始化向量,存储它们以便传输,接着使用 CreateEncryptor( ) 方法创建 ICryptoTransform 对象,再通过 CryptoStream 对象来执行加密转换,最后生成密文文本。实现核心代码如下:

```
ICryptoTransform RijndaelEnctypt =
  RijndaelProvider. CreateEncr - yptor( );
MemoryStream ms = new MemoryStream( );
CryptoStream cs = new CryptoStream( ms, RijndaelEnctypt,
  Crypto - StreamMode. Write);
cs. Write( Contract, 0, Contract. Length);
// Contract 为待加密合同
```

解密与加密的算法实现流程十分相似。此时需要将由 RSA 算法解密得到的会话密钥与初始化向量分配给 Key 与 IV 属性以供解密,并且使用 CreateDecryptor( ) 方法创建 ICryptoTransform 对象。实现核心代码如下:

```
ICryptoTransform RijndaelDecrypt = RijndaelProvider. CreateDecr -
  yptor( );
MemoryStream ms = new MemoryStream( EncContract, 0,
  EncCon - tract. Length);
// EncContract 为合同密文
CryptoStream cs = new CryptoStream( ms, RijndaelDecrypt,
  Crypto - StreamMode. Read);
```

数字签名的实施需要首先获取客户端本地证书存储区中的证书,其实现核心代码流程如图 4 所示。

数字签名验证的实施首先要加载发送者数字证书中的公钥,通过调用 Web 服务从服务器上获得,加载实现代码如下:

```
RSAParameters rsaKey = new RSAParameters( );
rsaKey. Modulus = PublicKey;                    //从服务器上获得
rsaKey. Exponent = Exponent;    //RSA 算法参数的 Exponent 值
rsa. ImportParameters( rsaKey);                 //公钥加载
```

然后将该公钥传递给 RSAPKCS1SignatureDeformatter 类的实例,使用 RSAPKCS1SignatureDeformatter. VerifySignature 方法验证签名。

应用 RSA 算法对 Rijndael 算法中会话密钥以及初始化向量加密,公钥加载方式与验证数字签名时相同,解密使用接收者本地存储区中数字证书的私钥,实现核心代码如下:

```
RSACryptoServiceProvider rsa = Mycert. PrivateKey as
RSACryptoServiceProvider;
//Mycert 为用户选择的证书
byte[ ] Para = rsa. Decrypt( RijndaelPara, false);
// RijndaelPara 为 KEY 或者 IV
```

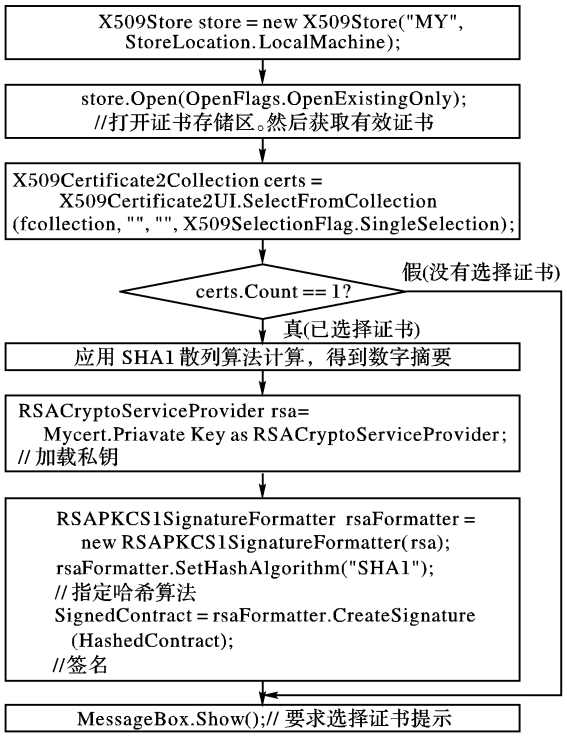

图 4 数字签名程序流程

3.3 智能客户端程序与网络洽谈模块登录者身份一致性实现

由上文分析而知,加密与数字签名子系统采用智能客户端构架。当企业方和商业方洽谈员通过洽谈达成一致后,需要传输电子合同,此时洽谈员必须首先通过该子系统对合同加密,并且进行数字签名。为了使加密与数字签名有效实施,必须确保实施加密、数字签名人员与网络洽谈模块当前洽谈员身份具有一致性。因此,智能客户端程序要求用户登录并且提供统一的数字证书。

实现方案如下:网络洽谈模块对洽谈员的信息进行记录。当用户访问智能客户端程序时,调用 Web 服务获取网络洽谈模块中当前洽谈员的信息与该用户信息进行核对,如果一致再对数字证书进行验证,否则拒绝登录。用户从本地证书存储区中选择数字证书,因为数字证书的序列号是唯一的,所以将该数字证书的序列号与其在网络洽谈模块中提供的数字证书序列号相比较,如果一致允许登录,否则拒绝。

4 结语

在微软. NET 环境下用 C#编码构建了网络采购系统的安全机制。通过双重身份认证方案解决了客户端与服务器身份认证、安全通信的问题,该方案根据系统的具体业务逻辑对客户端身份进行认证,既保证了业务逻辑的完整性也达到了其与数字证书的一致性。基于 B/S 模式下加密与数字签名的问题,通过智能客户端程序进行电子合同的加密和数字签名,实现了电子合同传输的机密性、完整性以及不可否认性,智能

(下转第 323 页)

2　安全性评估

现有的信息隐藏算法一般难以满足图像信息隐藏的理论安全条件,因此量化图像信息隐藏系统的实际安全强度是必要的,这对系统安全等级的划分和鉴别具有非常重要的现实意义。

2.1　评估方法

根据上述分析,在图像视觉特征可以有效约束的前提下,图像信息隐藏的安全性完全由其统计特征的变化程度来决定,统计特征的变化越大,安全性越差,相应的系统的安全等级越低。

文献[2]中证明了$\beta \geqslant 2^{-\varepsilon}$,因此可以用$\beta$的下限值作为系统安全等级划分的依据,即可用下式表示系统的安全性:

$$U = \begin{cases} 0 & \Delta S > T \\ \beta & \Delta S \leqslant T \end{cases} \tag{5}$$

其中$\beta = 2^{-D(p_{s_{i_1}s_{i_2}\cdots s_{i_{m-1}}} \| p_{c_{i_1}c_{i_2}\cdots c_{i_{m-1}}})}$。

利用式(5)进行安全等级的划分和鉴别,必须确定m,从理论上讲,m越大,所能约束的图像统计特征的阶数就越高,相应的对图像的安全性的评估就会越准确。

然而,实际计算中,m的取值却不宜过大。首先,从统计学的角度来看,利用统计假设检验理论必须已知载体的统计信息,其精度取决于样本容量大小。当以m个像素为载体时,载体空间的大小为$\prod_j^m JND_j$,对大小为$M \times N$的图像来说,可以获取的样本容量的大小为$M \times N$,因此当m增大时,样本容量相对变小。如果载体空间过大,样本容量相对较小时,就很难抓住稳定的统计规律,这样对载体的概率密度分布的统计会就会产生较大的误差,该误差可能远大于嵌入秘密消息所引入的误差,从而使评估对图像信息隐藏来说变得毫无意义。其次,图像各像素的强相关性表现为局部,即一般只有相邻的几个像素具有强相关性,它们与图像其他像素的相关性是较弱的,图像高阶统计特征是其弱相关性的表现形式,特征表现不明显,对它的成功检测需要高精度的隐写分析工具,阶数过高时检测已经是不可能,因此,m过大不仅不会改善运算精度,而且会大大增加运算的时间复杂。

2.2　LSB 算法的安全性

LSB 算法具有良好的视觉不可见性,因此只需以β值作为其安全等级划分和鉴别的依据。本节以 512 ×512 的 8 位灰度图像 lena. bmp 为例,针对不同的嵌入量和m,利用公式(5)对 LSB 算法的安全性进行评估,所得β值如表 1 所示。

表 1　LSB 算法的安全强度(嵌入率:bit/pixel)

m	嵌入率				
	1/16	1/8	1/4	1/2	1
1	1.0000	0.9999	0.9995	0.9984	0.9950
2	0.9974	0.9948	0.9883	0.9729	0.9436
3	0.9849	0.9700	0.9413	0.8981	0.8345

由表 1 可以得到以下几点结论:

1)m一定的情况下,嵌入量越大,系统的安全强度越低。增大嵌入量时,对图像统计特征的破坏程度相应增大,因此系统的安全强度下降。

2)嵌入量一定的情况下,m越大,对系统实际安全强度的量化越准确。m增大,式(5)中增加了对更高阶统计特性改变的量化,因此β值减小,更加接近系统安全强度的理论值。

表 2　不同 m 值下平均运算时间(t : S)

m	t
1	0.05
2	2
3	1000

不同m值下的平均运算时间如表 2 所示,m增大时,平均运算时间显著增大,且m取值很小时,平均运算时间已经很大。因此,继续增大m值,根据目前的算法难以对 LSB 算法的更高阶统计特征进行量化。

3　结语

信息隐藏对图像视觉特征和统计特征的破坏给隐写分析提供了依据,本文通过对图像载体视觉特征和统计特征的共同约束,得到了图像信息隐藏系统理论安全的充要条件,并给出了图像信息隐藏安全强度的测评方法。主要存在的问题是在安全性评估过程中,对参数m的确定尚未形成有效的方法,而且没有对统计分布产生的误差和忽略图像弱相关性所产生的误差进行量化,以至所得结果尚不精确,这些问题的解决还有待今后进一步的探讨和研究。

参考文献:

[1] 宋辉. 数据冗余空间中的掩密术安全性[J]. 中山大学学报(自然科学版), 2004,43(增刊):43 -46.

[2] CACHIN C. An Information - Theoretic Model for Steganography. Information Hiding[J]. Secoond International Workshop, 1998, 1525:306 -318.

[3] MOSKOWITZ IS. A New Paradigm in Steganography[J]. Proceedings New Security Paradigms Workshop, Sept. 2000:41 -50.

[4] 郭艳卿. 信息隐藏的层次安全性[J]. 中山大学学报(自然科学版),2004,43(增刊):56 -59.

[5] 林代茂. 图像的信息熵分析[J]. 中山大学学报(自然科学版),2004,43(增刊):89 -94.

[6] CHANDRAMOULI R. Steganography Capacity[J] . A Steganalysis Perspective Preceedings of SPIE, Security and watermarking of Multimedia Contents V. 2003, 5020: 173 -177.

[7] ZÖLLNER J. Modeling the Security of Steganographic Systems[J]. Information Hiding: Second International Workshop, 1998, 1525: 344 -354.

[8] 陈小勇. 几种典型的隐写系统安全性研究[D]. 南京: 南京理工大学,2004.

(上接第 320 页)

客户端程序不仅能够利用客户端本地资源完成加密和数字签名的工作,同时也能够克服传统客户端程序部署困难、管理困难的缺陷,为构造大型实用网络采购系统奠定了技术基础。

参考文献:

[1] THORSTEINSON P, GANESH GGA. . NET 安全性与密码术[M]. 梁志敏, 蔡建译. 北京: 清华大学出版社, 2004.

[2] KROWCZYK A. . NET 网络高级编程[M]. 吴旭超译. 北京: 清华大学出版社, 2003.

[3] 宋玲, 李陶深, 陈拓. 用 CAPICOM 组件实现应用系统安全性的方法[J]. 计算机工程, 2004, 30(16): 128 -130.

[4] 赵小明, 章美仁. DSA 数字签名技术在公文交换中的应用与设计[J]. 计算机应用与软件, 2005, 22(6): 142 -144.