企业数据信息交换的安全策略①

林碧英　吴　优 (华北电力大学 计算机科学与技术系 北京 102206)

摘　要： 在现代企业应用中，多个应用系统或者同一个系统的多个用户之间往往需要进行数据信息交换，如何保证数据传输中的安全变得越来越重要。讲述了如何利用 SSL 加密和 XML 加密保证数据交换安全的方案设计以及具体实现。并用实例予以了验证，有一定的实际意义。

关键词： SSL；XML；安全；加密；数据交换

Information Security in Enterprise Data Exchange

LIN Bi-Ying, WU You

(Department of Computer Science and Technology, North China Electricity Power University, Beijing 102206, China)

Abstract: In the Modern Enterprise Applications, data information needs to be exchanged between multiple application systems or between multiple users of a system. Therefore, it becomes more and more important to ensure the security of data transmission. The design of using SSL encryption and XML encryption to ensure the security of data exchange and its concrete realization are described in this paper. It is verified by some examples and of practical significance.

Keywords: SSL; XML ; security ; encrypt ; data exchange

1　引言

随着电子商务的发展，Internet 已经为众多的用户所认可和使用，越来越多的公司、企业和政府部门、科研单位选择通过 Internet 来传输数据和信息。由于 Internet 是一个基于 TCP/IP 协议的开放式互连网络，在享受其便利的同时，用户的数据资源便有被暴露的可能。而对于涉及到的国家政府、军事、文教等诸多领域，因为其中存贮、传输和处理的数据有许多是政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息，甚至是国家机密，如果被侵犯，则会在政治、经济等方面带来不可估量的损失。所以，在 Internet 上实现数据的安全传输就显得尤其重要。那么，如何保证数据在多个应用之间交换时的安全性，就成为基于互联网技术协同工作环境下需要解决的首要问题。数据交换的安全性体现在以下三个方面：数据传输的机密性、数据交换参与者的身份合法性、数据交换行为的不可抵赖性。

2　数据交换安全方案设计

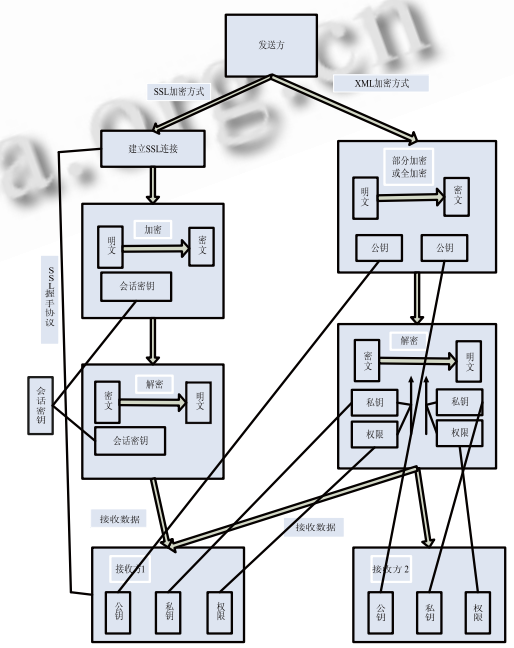

图 1　数据交换传输安全结构图

① 收稿时间:2009-07-20;收到修改稿时间:2009-08-17

本文以某企业为例，结合 SSL 加密技术和 XML 加密技术，确保数据在交换传输的过程中不被黑客拦截并进行破解，进而导致数据泄露。下面分别介绍 SSL 加密、XML 加密的相关原理和具体模块的设计。其逻辑图如图 1 所示。

2.1 SSL 加密

2.1.1 SSL 加密功能

SSL 加密是在安全的传输通道中进行消息的传递，可以保证客户机和服务器通信的安全，满足数据交换的及时性。

2.1.2 SSL 加密原理

SSL 协议[1]使用不对称加密技术实现会话双方之间信息的安全传递。可以实现信息传递的保密性、完整性，并且会话双方能鉴别对方身份。

不同于常用的 http 协议，在与网站建立 SSL 安全连接时使用 https 协议，即采用 https://ip:port/的方式来访问。当与一个网站建立 https 连接时，浏览器与 Web Server 之间要经过一个握手的过程来完成身份鉴定与密钥交换，从而建立安全连接。

2.2 XML 加密

2.2.1 XML 加密功能

主要完成多方(不止两方)之间的安全会话和加密交换数据的一部分或整个文档。

在设计中，可以对整个 XML 文档进行加密，可以对一个元素及其所有子元素进行加密，可以对一个 XML 文档的内容部分进行加密，也可以对 XML 文档外部资源的引用进行加密。可以在企业数据交换中交换安全的和非安全的数据，使不同权限的用户只能看见相关部分的数据。

2.2.2 XML 加密原理

XML 加密技术可以利用数字证书对整篇或部分 XML 文档进行加密，实现不同数据使用不同密钥进行加密的多方数据交换，即可以采用 A 的密钥对 A 感兴趣的部分进行加密，而使用 B 的密钥对 B 感兴趣的部分进行加密。在数据交互处理过程中，不同的参与者只能操作与之相关的部分，而无法看到其它部分，从而保证了数据在多方处理、传递过程中的安全性。

XML 加密语法的核心元素是 EncryptedData[2]元素，该元素与 EncryptedKey 元素一起用来将加密密钥从发起方传送到已知的接收方，EncryptedData 是从 EncryptedType 抽象类型派生的。要加密的数据可以是任意数据、XML 文档、XML 元素或 XML 元素内容；加密数据的结果是一个包含或引用密码数据的 XML 加密元素。当加密元素或元素内容时，EncryptedData 元素替换 XML 文档加密版本中的该元素或内容。当加密的是任意数据时，EncryptedData 元素可能成为新 XML 文档的根，或者成为一个子代元素。当加密整个 XML 文档时，EncryptedData 元素可能成为新文档的根。此外 EncryptedData 不能是另一个 EncryptedData 元素的父代或子代元素，实际加密的数据可以是包括现有 EncryptedDat 或 EncryptedKey 元素的任何内容，加密的颗粒度可以根据具体要求的不同而不同。

3 数据交换安全方案具体实施

由于企业数据交换需要提供多种交换方式，以满足不同应用场景的交换需要。按照交换的数据量和及时性要求，需要提供同步和异步的交换方式；从交换的发起方区分，需要提供发送和抽取方式；从交换的触发源区分，需要提供应用触发和自动方式。这里重点讲同步和异步的安全交换方式。交换包括发送方处理、数据传输、接收方处理三个过程，同步是这三个过程按顺序全部执行完成后，发送方才收到反馈，在此过程中，发送方一直处于阻塞状态；异步是发送方处理完成后就返回，而数据传输、接收方处理都在后台进行。同步适合于数据量较小，及时性要求较高的交换需求；异步适合于数据量较大的交换需求。

3.1 同步交换

由于在企业的数据交换过程中，比如像日报等一些紧急的文档，需要接受方能立即接收到发送方发送过来的文件并做出回应，及时性要求很高， 这时选择 SSL 加密，确保双方都在线，并且能及时发送消息和文件，从而保证工作的顺利进行。

3.2 异步交换

由于在企业的数据交换过程中，比如像季报、年报等一些不那么紧急的文档，只要能接收到发送方发送过来的文件即可，及时性要求不高。

3.3 模块实现

本系统在保证数据交换安全性的过程中，可以根据任务的及时性、紧迫性、权限等，选择合适的加密方式。发送方在发送加密文件过去后，根据发送的文件标记上是采用的 SSL 加密还是 XML 加密，接收方在

接收到文件后自动选择解密的方式。

3.3.1 服务器端实现

服务器端的实现主要分为二个模块：SSL 加密和 XML 加密。下面重点介绍 XML 加密模块。

若选择 XML 加密，应先生成指定的 EXCEL 模板，在模板填写数据并保存，然后将其转化为 XML 格式，然后选择对整个文档加密还是部分加密，最后发送到接收方的服务器上的某一个指定的文件夹，同时在接收方会提示请接收某某文件，接收方通过对加密后的 XML 文件解密得到原文件。其中采用的关键技术是 XML 全加密技术，部分加密技术，XML 签名技术，如何用程序创建 EXCEL 文件和如何将 EXCEL 文件转化为 XML 文件。其实现效果如图 2 所示。

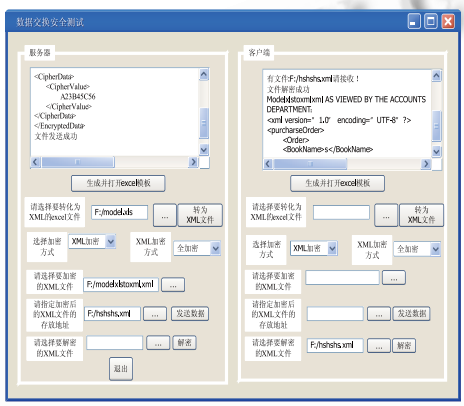

图 2　XML 加密实现效果

XML 全加密技术 :例如清单 1(要加密的样本 XML 文件)，其中包括订购信息 Order 和付款信息 Payment，这时图书销售商对整个 XML 文件加密，以产生 XML 加密的文件，这样就可以发送到出版社的销售部门。清单 2 是对整个 XML 加密后的 XML 文件，其中实际加密的数据作为 <CipherValue> 标记的内容出现。整个 CipherData 元素出现在一个 EncryptedData 元素内[3]。

EncryptedData 元素包含用于加密的 XML 名称空间。虽然这种方法在端对端通信链路中提供了适当的安全性，但违反了图书销售商的安全性策略。该策略要求不透露销售部门的支付信息而向会计部门提供该信息。在这种情况下，销售部门对整个 XML 文档解密，这就泄露了支付信息。

XML 部分加密技术：对于清单 1 中，图书销售商不想让销售部门看见付款信息 Payment，这时图书销售商可以用会计部门的秘钥对 XML 文件的支付信息部分加密，而使文件内容其余部分保持不加密，以便销售部门查看。清单 3 为对付款信息加密后的 XML 文件，可以看见 XML 文件中的订购付款信息 Order 没有加密，而付款信息 Payment 中的元素已经被加密，这样信用卡信息也变得安全，因为它驻留在加密的 Payment 元素的子节点中。由于安全性要求规定必须对未授权的查看者保密支付方式(诸如信用卡或银行支票)，对 Payment 元素加密就做到了这一点。

(1) 清单 1：(要被加密的样本 XML 文件，这个 XML 文件包括订购信息 Order 和付款信息 Payment，其中 Order 节点下包括订购书名 BookName、订购书号 ItemId 和订购数量 Quantity，Payment 节点下包括卡号 CardId、卡名 CardName 和有效日期 ValiDate。)

```
<purchaseOrder>
<Order>
  <BookName>book</ BookName >
  < ItemId>123-958-74598</ ItemId>
  <Quantity>12</Quantity>
</Order>
<Payment>
<CardId>123654-8988889-9996874</CardId>
  <CardName>visa</CardName>
  <ValidDate>12-10-2004</ValidDate>
</Payment>
</purchaseOrder>
```

(2) 清单 2：(对整个文档加密后的 XML 文件，其中只包含了加密模式，实际加密的数据作为 <CipherValue> 标记的内容出现，EncryptedData 元素包含用于加密的 XML 名称空间，属性 xmls 指定了用来加密 XML 数据的 XML 加密名称空间。属性 Type 用来对 XML 的类型定义。)

```
<?xml version='1.0' ?>
<EncryptedData
xmlns='http://www.w3.org/2001/04/xmlenc#'
  Type='http://www.isi.edu/in-notes/iana/assignments/media-types/text/xml'>
  <CipherData>
  <CipherValue>A23B45C56</CipherValue>
```

```
    </CipherData>
  </EncryptedData>
```

(3) 清单 3：(对部分文档加密后的 XML 文件，其中包含XML加密模式又包含来自清单1中原始数据的元素 Order 订购信息，另外清单 1 中元素 Payment 付款信息已被加密，片段#Element 表示一个EncryptedData—这代表一个元素。)

```
<?xml version='1.0' ?>
<PurchaseOrder>
  <Order>
    < BookName >book</ BookName >
    <ItemId>123-958-74598</ ItemId >
    <Quantity>12</Quantity>
</Order>
<EncryptedData
Type='http://www.w3.org/2001/04/xmlenc#Element'
  xmlns='http://www.w3.org/2001/04/xmlenc#'>
    <CipherData>
    <CipherValue>A23B45C564587</CipherValue>
    </CipherData>
    </EncryptedData>
</PurchaseOrder>
```

3.3.2 客户端实现

客户端的实现和服务器端的实现区别在于 SSL 加密时候，客户端不能启动 SSL 连接，只有在服务器端启动 SSL 连接，客户端才能连接上服务器。在服务器端没有启动 SSL 安全连接的时候，客户端就只能采用异步方式的 XML 加密，其他的设计和实现都类似服务器端。

4 结论

传统的企业的数据交换安全解决方案是采用 SSL 技术。然而，在多个应用协同工作的环境中，往往会产生“多方(不止两方)安全会话”的问题，例如：商家可能需要知道客户的名称和地址，但不应当知道任何关于信用卡的详细信息，而银行不需要了解客户购买货物的详细信息，却必须知道其信用卡信息。这种情况下，需要对数据的不同部分使用不同的密钥和方法进行加密和签名，而采用传统的基于 SSL 技术的方案无法实现对数据部分加密和签名，也就难以保证多方数据交换的安全性。这时可以 PKI 安全体系为基础[4]，结合 XML 加密和签名技术，解决多方安全会话问题，满足企业对协同工作中多方数据交换的安全要求。另外，由于 SSL 复杂的认证方案和加密解密算法，需要大量消耗 CPU 资源，从而造成服务器性能有所降低。因此在实际运用中要根据需要对安全强度和程序的性能加以权衡。但是 XML 加密无法做到 SSL 协议那样的及时性要求，所以在本文中结合二者的优缺点来保证企业数据交换过程中的安全性和及时性。

参考文献

1 ShoriakTimothyG SSL/TIS Protocol Enalble ment for Key Recover , Computer and Security, 2000,19.

2 Eastlake D, Reagle J. XML Encryption Syntax and ProcessingW3C Recommendation [2002-12-10]. http://www.w3.org/TR/xmlenc-core.

3 Bilal Siddiuqi.探索 XML 加密,第 1 部分[2002-03-01] http://www-128.ibm.eom/developerworks/en/xml/x-encrypt/index.html

4 Myers M, et al, RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate status protocol-OCSP, June 1999, http:// www1etf.org/rfc/RFC2560.txt.