数字签名在电子军务系统中的实现

寇雅楠，　邢国强，　吴成波，　宋翔宇

(空军工程大学工程学院，陕西西安 710038)

摘　要：阐述了数字签名的基本原理，探讨了如何用数字签名来保证电子军务系统中公文流转的完整性、抗否定性、以及身份验证机制。提出了一种基于数字签名的电子军务公文流转系统，并依赖于Java2安全体系在J2EE平台上予以实现。该系统实现了有效确认发文方身份并防止了他人对网上所传输文件的破坏。

关键词：数字签名；电子军务；RsA算法；J2EE

中图分类号：TP393.　08　　**文献标识码**：A　　**文章编号**：1009-3516(2006)05-0045-03

电子军务是传统军事业务的电子化，是军队信息化建设的一个新领域和重要目标。而网络具有的开放、共享、交互等特点，决定了电子军务应用不可避免地存在着信息安全隐患。同时，由于军队的特殊性，一切行为必须要求具有高度的可靠性和安全性。因此在电子军务系统上传输的信息数据必须具有抗否定性、安全性、以及身份验证机制。数字签名正是基于这些特性建立起来的一种机制，无疑会在电子军务系统得到广泛应用。目前，研究信息传输加密的算法较多，但针对电子军务系统的却较少[1-4]。

J2EE是Java2的企业应用版本，在Java 2 SDK 1.5中更是集成了JCE、JSSE、和JAAS等Java安全扩展平台。这些安全机制在开发基于数字签名的军队电子政务系统中具有极强的适用性[5]。

1　RSA公钥加密与数字签名

RSA算法是最广泛使用的公钥加密算法之一。以私钥作为加密密钥，公钥作为解密密钥，可以实现1个用户加密的消息使多个用户解读，用于数字签名。RSA作为公钥密码体制是利用了单向陷门函数原理[6]。

RSA算法的安全性依赖于大整数分解难题，即如何将n因式分解为2个素数。对值很大的n来说，因式分解是很难的。所以，RSA需采用足够大的素数。因式分解越困难，密码就越难以破译，加密强度就越高。

数字签名用来确定数据的来源。数字签名的基础是基于公钥和私钥的非对称加密，发送者使用私钥加密消息摘要，得到数字签名，接收者使用公钥解密数字签名确定是否是某个人发送的。

在RSA签名体制中，把需要签名的消息M作为一个散列函数输入，由此输出一个定长的安全散列码。发送方用自己的私钥Kprk将这个散列码进行加密就形成签名。此后，将消息M和签名传送出去。接收方接受到消息M，根据消息M计算一个散列码，同时使用发送的公钥Kpbk对签名进行解密。若解密后的散列码和计算得出的散列码一致，则签名是有效的。因为只有发送方知道自己的私钥，所以，只有发送方才能生成合法的签名。

2　数字签名在电子军务系统中的实现

军队内部管理自动化是电子军务的基础。内部管理自动化的主要目标是实现办公无纸化和内部网络化，提高军队内部事务处理能力和军队管理效率。在电子军务中，要真正实行无纸化办公，很重要的一点是

收稿日期：2005-10-31
作者简介：寇雅楠(1964-)，女，陕西三原人，副教授，博士，主要从事计算机网络安全研究.

实现电子公文的流转。因为电子军务的所有活动都是军队行为,要求具有高度的可靠性和安全性,所以除了传统的身份认证与识别、访问控制、信息加密等技术外,很重要的一点是如何防止他人对网上所传输的文件的破坏,以及如何确认发文方的身份。数字签名技术这种能保证数据的完整性、机密性、抗否定性的信息安全技术是保障军队公文网上传输完整性和不可抵赖性的主要技术手段之一。

在电子军务公文流转系统中,做以下设计:服务器拥有密钥库,保存各个用户的公钥,并分发给各个用户对应的私钥;公文发送方 A 首先用自己的私钥 Aprk 对待发送的公文进行数字签名,然后使用 SSL 协议与服务器进行加密通信,将待发送的公文和数字签名加密发送给服务器;公文接收方 B 要接收公文时,首先也使用 SSL 协议与服务器加密通信,安全获取公文,然后要求服务器用发送方对应的公钥 Apbk 对数字签名进行验证,并获取验证结果。

此系统在 J2EE 平台上用 Java 语言具体实现的核心部分如下:

1)服务器产生密钥对,私钥分发给用户,公钥保存在密钥库中:

包含在 java. security 中的 KeyPairGenerator 类提供了创建密钥对以用于非对称加密的方法:

KeyPairGenerator kpg = KeyPairGenerator. getInstance("RSA");

参数为 RSA,指定了非对称加密所使用的方法;

kpg. initialize(1024);

初始化密钥生成器,指定密钥长度为 1024 位;

KeyPair kp = kpg. genKeyPair();

生成密钥对,包含了一对公钥和私钥信息;

PublicKey pbkey = kp. getPublic();

PrivateKey prkey = kp. getPrivate();

获取公钥和私钥。

2)公文发送方用自己的私钥对待发送的公文进行数字签名,然后使用 SSL 协议将待发送的公文和数字签名发送给服务器:

假设待发送的公文为 data. doc,通过文件输入流将其读入字节类型数组 data 中,发送方私钥保存在 prk. dat 文件中,通过文件输入流读入私钥存放在 RSAPrivateKey 类型的变量 prk 中;

javax. security 包中的 Signature 类提供了进行数字签名的方法:

Signature s = Signature. getInstance("MD5WithRSA");

获取 Signature 对象,参数中包含了计算消息摘要所用的算法和加密消息摘要所用的算法;

s. initSign(prk);

用发送方的私钥初始化 Signature 对象,将使用此私钥加密消息摘要;

s. update(data);传入要签名的数据,即待发送的公文;

byte signeddata[] = s. sign();

执行签名,返回字节数组;

发送方与服务器建立好 SSL 通信后,就可以将待发送公文和数字签名传送给服务器。

3)当公文接收方接收公文时,服务器对数字签名进行验证,并把验证结果传给接收方:

服务器从密钥库中获取公文发送方的公钥,并存放在 RSAPublicKey 类型的变量 pbk 中;

Signature s = Signature. getInstance("MD5WithRSA");

获取 Signature 对象;

s. initVerify(pbk);

用发送方公钥初始化 Signature 对象,将使用此公钥解密消息摘要;

s. update(data);传入从发送方获取的公文数据;

boolean authorized = s. verify(signeddata);

验证从发送方获取的数字签名 signeddata,返回布尔类型的验证结果;

当公文接收方与服务器建立好 SSL 通信后,服务器就可以把公文和数字签名验证结果传送给接收方。

3　结束语

电子军务是军队信息化建设的一个新领域和重要目标。基于军队活动具有高度保密性和安全性的要求,本文分析了非对称加密算法,提出了一种基于数字签名的电子军务公文流转系统,并在J2EE平台上加以实现。此系统有效地确认发文方的身份并防止他人对网上所传输的文件的破坏。数字签名技术这种能保证数据的完整性、机密性、抗否定性的信息安全技术将成为保障军队公文网上传输完整性和不可抵赖性的主要技术手段。

参考文献:

[1] 肖　蕾. 基于Jawa的数字签名技术在电子政务中的应用[EB/OL]. WWW. achit. com. 2006 - 01 - 21.
[2] 王晓东,郑连清. 一种具有身份认证功能的微型邮件引擎[J]. 空军工程大学学报(自然科学版),2003,4(4):48 - 52.
[3] 欧阳中辉,郝明涛,薛　锋. Intranet信息安全若干问题及应对措施[J]. 海军航空工程学院学报,2004,19(2):243 - 245.
[4] 朱根标,张风鸣,王金干. 一种PE文件RSA验证加密算法[J]. 空军工程大学学报(自然科学版),2005,6(4):67 - 69.
[5] Li Gong,Gary Ellison,Mary Dageforde. Inside Java2 Platform Security[M]. 北京:电子工业出版社,2004.

(编辑:姚树峰)

The Application of Digital Signature in the Electronic Military Affairs

KOU Ya - nan, XING Guo - qiang, WU Cheng - bo, SONG Xiang - yu

(The Engineering Institute, Air Force Engineering University, Xi'an 710038, Shaanxi, China)

Abstract: This article elaborates the basic principle of digital signature, and discusses how to use this technology to ensure the integrity, authenticity and non - deny in the file transfer system of electronic military affairs. Finally, this article gives a model of file transfer system based on the digital signature technology, and makes it realized based on J2EE platform by using Java2 security system. This digital signature ensures the integrity and confidentiality to the file.

Key words: digital signature ; electronic military affairs; RSA algorithm ; J2EE

(上接第44页)

[6] 杨　策,张永智,庞正社. 网络流量监测技术及性能分析[J]. 空军工程大学学报(自然科学版),2003,4(1):57 - 60.

(编辑:门向生)

Research for the GPON Dynamic Bandwidth Allocation Algorithm Based on Wavelet

CHEN Fu - du1, LI Wei - min1 , ZHANG Chun - min2, ZHANG Li -juan1

(1. The Communication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China;
2. The Science Institute, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: With wavelet, Long Range Dependence can be converted into Short Range Dependence and the network traffic can be predicted. Then the result can be applied to the GPON Dynamic Bandwidth Allocation. Finally, an improved dynamic bandwidth allocation algorithm is proposed.

Key words: Gigabit- capable passive optical network (GPON) ; dynamic bandwidth allocation (DBA) ; wavelet; long range dependence; short range dependence