第 36 卷　第 20 期　　计　算　机　工　程　　2010 年 10 月
Vol.36　No.20　　Computer Engineering　　October 2010
·安全技术·　文章编号：1000—3428(2010)20—0131—03　文献标识码：A　中图分类号：N945

基于 OpenSSL 的航行情报信息安全研究

吴志军，黄　俊，石　贞
(中国民航大学电子信息工程学院，天津　300300)

摘　要：结合 CAAC 骨干异步传输 ATM 网的体系结构，并根据航行情报信息传输的过程，在分析报文组成和格式的基础上，提出一种基于 OpenSSL 的航行情报信息安全的保护方法，研究航行情报信息安全保障的关键技术，实现空中交通管理 ATM 业务数据加密和数字签名技术，从而保障了航行情报信息的机密性、完整性、有效性和实时性。

关键词：民航；航行情报信息；数据加密；数字签名

Research on Aeronautical Information Security Based on OpenSSL

WU Zhi-jun, HUANG Jun, SHI Zhen
(School of Telecommunication and Engineering, Civil Aviation University of China, Tianjin 300300, China)

【Abstract】 This paper advances a method to ensure aeronautical information safely based on OpenSSL according to ATM network architecture of CAAC and the process of aeronautical information transmission. It researches the key technology about protecting aeronautical information, implements the encryption and digital signature technology, protects the aeronautical information confidentiality, integrity, availability and real-time.

【Key words】 civil aviation; aeronautical information; data encryption; digital signature

1　概述

随着航空事业的发展，航班越来越多，飞行的密度越来越大，各种信息的交流以及处理越来越多。空中交通管理(Air Traffic Management, ATM)中的信息数据面临安全威胁越来越大，同时也存在一定的安全隐患，不利于飞行安全。为了保证飞行安全，针对互联网上的黑客攻击、信息泄密和病毒泛滥问题，空管信息化管理和实施部门采取了严格的管理措施和技术手段来保护空管信息资源，并在一定程度上保证了空管信息化系统没有发生严重的信息安全事故。同时又可以为航空公司、机场等民航单位，甚至为社会公众提供信息服务，创造社会效益和经济价值。

虽然目前国内的信息化系统已经采取了管理措施和技术手段进行了初步的网络信息安全建设工作，但是与国外空管行业以及国内先进行业的信息安全建设相比还存在一定的差距。人们急需在空管信息化网络中建设一套完善的信息安全保障体系，以保证空管信息系统的安全运行。近年来，由于信息安全事件多次导致民航大面积航班的延迟和取消，给人们生活带来了诸多不便。为了减小信息安全事件给航空交通运输带来的影响，根据国际民航组织(International Civil Aviation Organization, ICAO)的要求，必须对航空运输的信息采取安全措施，因此，民航总局将 2007 年定为“信息安全年”，计划针对包括 ATM 业务数据在内的航空信息进行安全保障[1]。

2　相关工作

目前，中国民航 CAAC(Civil Aviation Administration of China)的业务信息数据并未采用任何保障措施，而针对这方面安全性的研究也几乎为空白。本文的主要内容是基于 OpenSSL 的航行情报信息安全的研究，利用 OpenSSL 提供的 TLS/SSL 编程接口对 ATM 业务数据进行数据加密和数字签名，以保障航行情报(Aeronautical Information, AI)的数据安全。

3　航行情报信息的安全方案

总局情报中心与各地区二级情报中心可以通过 ATM 进行联结，也可以通过 AFTN(Aeronautical Fixed Telecommunication Network)网连接；二级节点与三级节点之间则只能通过 AFTN 网络进行连接[2]，民航空管情报网络系统拓扑图如图 1 所示。

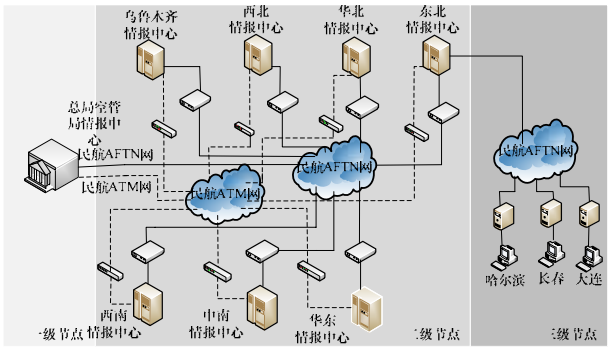

图 1　情报网络互联系统拓扑

根据航行情报的网络拓扑结构，采用的数据加密技术主要是对传输中的数据流进行加密，数据在发送端进行加密，在接收端进行解密，实现民航总局与地区空管局、地区空管局之间的信息互联，CA(Certificate Authority)服务器则实现总

基金项目：国家自然科学基金与中国民用航空总局联合基金资助项目(60776808)；天津市应用基础及前沿技术研究计划基金资助项目(09JCYBJC00400)

作者简介：吴志军(1965－)，男，教授、博士生导师，主研方向：网络信息安全；黄　俊、石　贞，硕士研究生

收稿日期：2010-02-10　**E-mail：**caucwu@263.net

局和地区空管局证书的颁发和查询。以一级节点与二级节点的连接关系进行说明，在民航总局进行数据加密和数字签名，将加密的信息传输到地区空管局，然后在地区空管局进行数据的验证数字签名和解密，这样就增加了民航总局与地区空管局之间信息传输的安全性。同样，各地区空管局也可通过数据加密和解密的方法实现各地区空管局之间信息的安全保障。具体的方案如图 2 所示，数据加密和数字签名技术的具体实现流程如图 3 所示。

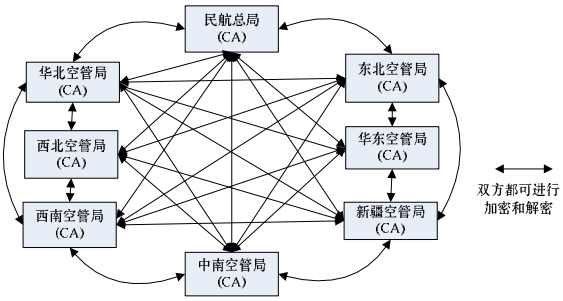

图 2　信息安全保障方案

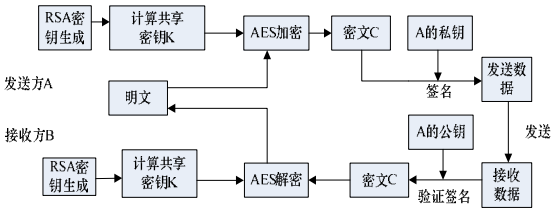

图 3　加密签名、验证解密流程

4　航行情报信息安全的关键技术

本文在航行情报信息安全问题上采取了一种基于 AES 和 RSA 的混合密码体制对数据进行加密。而在信息摘要和数字签名技术上，本方案采用 SHA1 算法对数据进行信息摘要，用 RSA 算法进行数字签名。下面就本文采用的安全技术进行介绍。

4.1　数据加密技术

先介绍基于 AES 和 RSA 的混合密码体制。针对航行情报网的网络结构，提出了一套混合加密体系来保证数据在 ATM 网络中传输的安全性。在混合密码体制中提出一种基于网状的密钥协商方案，在这个方案中，八大空管局的互联成网状，它们共享一对大素数，分别独立产生秘密数值并计算中间值，然后把这些中间值按互联方式传递给其他空管局，最后每个空管局都可以利用这些中间值和自己的秘密数值计算出群密钥，即共享密钥 K，并用 K 进行 AES 算法。

在进行数据加密和数字签名技术时，用到了功能强大的 OpenSSL 软件包。由于我国民航普遍运用 Unix(Linux)系统，因此选择在 Linux 系统下安装和编译 OpenSSL 软件，并建立基于 OpenSSL 的 CA 服务器。在建好 CA 服务器后，可以使用 OpenSSL 的指令对发送端的数据进行加密或数字签名[3]。

以民航总局和华北空管局为例，发送方为 A，接收方为 B，数据加密技术的具体实行步骤如下：

(1)通信时首先公开一个大素数 P 和本原元 g，A 向 CA 申请一对 RSA 密钥，设私钥为 x_a，将计算值 $y_a = g^{x_a} \bmod p$ 发送给 B；

(2)B 向 CA 申请一对 RSA 密钥，设其私钥为 x_b，将计算值 $y_b = g^{x_b} \bmod p$ 发送给 A；

(3)A 计算会话密钥：$k_a = y_b^{x_a} \bmod p = g^{x_b x_a} \bmod p$，B 也得到会话密钥：$k_b = y_a^{x_b} \bmod p = g^{x_a x_b} \bmod p$。这样 A、B 就获得只有他们知道的共享密钥 K；

(4)用共享密钥 K 对数据进行 AES 算法。

AES 算法由 OpenSSL 指令完成[3]：

OpenSSL>aes-128-cbc–in pln.txt–out enc.txt–kfile sharekey.pem –e–a;

其中，sharekey.pem 为编程计算所获得的共享密钥。

本方案中共享密钥的计算由编程实现如下：

程序 1[4-7]：

```
{
DH        *d1,*d2;
          BIO       *b;
          int          ret,size,i,len1,len2;
          charsharekey1[128],sharekey2[128];
          /* 构造 DH 数据结构 */
                d1=DH_new();
          d2=DH_new();
            /* 生成 d1 的密钥参数，该密钥参数是可以公开的 */
 ret=DH_generate_parameters_ex(d1,64,DH_GENERATOR_2,NULL);
/* 检查密钥参数 */
ret=DH_check(d1,&i);
             /* p 和 g 为公开的密钥参数，因此可以拷贝 */
          d2->p=BN_dup(d1->p);
          d2->g=BN_dup(d1->g);
ret=DH_generate_key(d1);
ret=DH_generate_key(d2);
/* 计算共享密钥 */
      len1=DH_compute_key(sharekey1,d2->pub_key,d1);
      len2=DH_compute_key(sharekey2,d1->pub_key,d2);
        if((len1==len2)&&(memcmp(sharekey1,sharekey2,len1)==0) )
                printf("生成共享密钥成功\n");
       b=BIO_new_file(“/home/test/sharekey.pem”，”w”)；
        PEM_write_bio(b,”SHARE
KEY TEST”,”APPENDING”,sharekey1,128);
        }
```

4.2　信息摘要与数字签名技术

以上混合密钥加密方案中有一个固有的弱点，难以进行身份认证，也无法避免插入重放攻击[8]。第三方可以伪装成 A 方向 B 方传送信息，也可以轻易地截取信息，进行修改后再发送给 B 方。B 方如何确定信息是 A 方发送的并保证信息是完整的呢，为了解决这个问题，必须采用信息摘要和数字签名技术。

本方案采用 SHA1 算法进行信息摘要，SHA1 是一种用于数字签名的安全散列算法，当输入消息其长度小于 2^{64} 位时，即消息填充为 512 位的整数倍时，SHA1 产生一组 160 位的杂凑值输出，将此杂凑值输入到数字签名的算法中(如 RSA)。杂凑值用于签名，可大大提高数字签名的速度，因为杂凑值比通常的消息小得多。

因此，本方案就采用具有杂凑值的数字签名技术，采用 SHA1 算法产生一组杂凑值，然后对杂凑值进行 RSA 加密算法，得到数字签名，然后将原文和数字签名一起发送给接收方，接收方用发送方的公钥进行验证，最后与原文进行比较。数字签名在信息安全中，如身份认证、数据完整性、数据保密性及不可否认性等方面起重要作用[8]。

具体的信息摘要和数字签名技术的实现如下[3]：

发送方 A：

OpenSSL>req–new–newkey rsa:1024 –keyout privkey.pem–out req.pem–passout pass: 123456 (生成证书请求和密钥)

OpenSSL> ca –in req.pem out cert.pem (发布证书)

OpenSSL> rsa –in privkey.pem –passin pass:123456 –out pubkey.pem –pubout (根据私钥导出相应的公钥)

OpenSSL> sha1 –sign privkey.pem –out sgn.txt enc.txt

(信息摘要和数字签名)

将 sgn.txt、enc.txt、pubkey.pem 一起发送给 B。

接收方 B：

OpenSSL> sha1 –verify pubkey.pem –signature sgn.txt enc.txt

(验证签名)

5 结果分析

现今，国内的民航业务信息系统并未采取任何加密技术来保证数据的安全性，因此，本文所提出的混合加密体制有一定的可行性，数据加密和数字签名的实验结果如表 1 和表 2 所示(以任一字符为例)。

表 1 数据加密的实验结果

原文件	共享密钥 K(PEM)	AES 加密后的密文 enc.txt
hello!	KSzudAW40zj0f5UApmZmAIzLZgC4rfG/boqEAIzLZgA8v4AAQMX4t8it8b+ArvG/WAaAAE2EBAigwvi3AK7xvzggfwAuTj32AAAAAAAAAAABAAAAAAAAAKu6/QAAAAAyL8OBgEAAABl7YIANgELBqDC+LfAhgQIOK5PUIieBAg=	U2FsdGVkX19kgrsTI0NnHDdRjkcTJVB1RLnvYippbUo=

表 2 数字签名的实验结果

信息摘要后的密文	信息摘要和数字签名后的密文	验证、解密后的文件
SHA1(enc.txt)=99e4b41c47cdf6c55d309feb479f1865fa0d7d62	不可识别字符	hello!

6 安全性分析

(1)机密性

本文采用的混合密码体制的核心思想就是大素数不可分解质因数的数学理论方法。由于共享密钥 k_b 和 k_a 是相同的，$K=k_a=(y_b)^{x_a}=\left(a^{x_b}\right)^{x_a}=k_b=(y_a)^{xb}=\left(a^{xa}\right)^{xb}$，那么攻击者必须知道 x_a 和 x_b 才能得到共享的密钥 K，而公开的信息只有 y_a 和 y_b，由离散对数问题，从 y_a 和 y_b 中求出 x_a 和 x_b 在计算上是不可行的，这保证了算法的安全性。相对 DES 算法，AES 算法的实现更简单。同时由于 AES 算法具备很强的扩散性能，最终形成的密码有很高的随机性，抗分析攻击能力强。AES 设计有 3 个密钥长度：128 位，192 位，256 位，相对而言，AES 的 128 位密钥比 DES 的 56 位密钥强 1 021 倍。

(2)完整性

该方案的密文是采用 SHA1 进行信息摘要，它的特性是不可以从消息摘要中复原信息，并且 2 个不同的消息不会产生同样的消息摘要。因此，可以很好地体现数据的完整性。

(3)有效性

该方案采用 RSA 算法进行数字签名，到 2008 年为止，世界上还没有任何可靠的攻击 RSA 算法的方式。只要其钥匙的长度足够长，用 RSA 加密的信息实际上是不能被破解的。因此，签名不易被改动，可以保证数据的有效性。

(4)实时性

AES 算法设计简单，密钥安装快、需要的内存空间少，在所有平台上运行良好，支持并行处理，还可抵抗所有已知攻击，所以 AES 在具有比三重 DES 更强安全系数的同时，还保证了相比三重 DES 的更高的加解密效率，这就大大提高了信息加密速度。此方案采用的 AES 的密钥长度是 128 位，加密后密文长度不会大幅度增加，因此，不会影响信息数据在网络中的传输速度，从而在加密效率和传输效率两方面保证了数据的实时性。

(5)OPENSSL 安全漏洞的应对

作为 OpenSSL Project OpenSSL 0.9.8i 或者更低的版本，存在以下 2 个漏洞报告，攻击方可以利用此漏洞进行 DoS 攻击：(1)library 没有数量限制的缓冲 Datagram TLS 记录，通过特制的 Datagram TLS 包而达到用尽所有可用内存的目的。(2)Datagram TLS 出现错误信息处理，可派遣大量的顺序握手消息而达到用尽所有可用内存的目的。

解决方案是升级到版本 OpenSSL Project OpenSSL 0.9.8k 或者登录 Openssl CVS Web Interface 检查以下文件的本地版本的升级修改：

openssl/ssl/d1_both.c(1.14.2.8 -> 1.14.2.9)

openssl/crypto/pqueue/pqueue.c(1.2.2.4->1.2.2.5)

openssl/crypto/pqueue/pqueue.h(1.2.2.1 -> 1.2.2.2)

openssl/ssl/d1_pkt.c(1.4.2.17 -> 1.4.2.18)。

7 结束语

本文提出一种基于 OpenSSL 的航行情报系统的安全保障方案，成功构建了 CA 服务器，使用了密钥交换算法计算共享密钥，对航行情报明文数据进行 AES 数据加密，然后使用 SHA1 和 RSA 算法，对航行情报数据进行信息摘要和数字签名，最终实现在非安全信道环境下航行情报信息通信的认证、完整性、机密性和实时性。

参考文献

[1] 张 军. 现代空中交通管理[M]. 北京: 北京航空航天大学出版社, 2005.

[2] 刘 勇. 航行情报动态信息系统的设计[D]. 西安: 西安电子科技大学, 2005.

[3] 王志海, 童新海, 沈 寒. OpenSSL 与网络信息安全——基础、结构和指令[M]. 北京: 清华大学出版社, 2007.

[4] 赵春平. OpenSSL 编程[EB/OL]. (2007-08-18). http://download.csdn.net/source/427435.

[5] William S. Cryptography and Network Security: Principles and Practice[M]. 2nd ed. Beijing, China: Publishing House of Electronics Industry, 2001.

[6] Schneier B. 应用密码学:协议算法和 C 源程序[M]. 北京: 机械工业出版社, 2002.

[7] 徐扛峰, 赵 蜂. 基于双密钥的对称加密方案[J]. 计算机工程, 2008, 34(8): 133-134.

[8] 关振胜. 公钥基础设施 PKI 及其应用[M]. 北京: 电子工业出版社, 1992.

编辑 陈 文