无线安全中间件的设计与应用

Design and Application of Wireless Security Middleware

江 颉 蒋融融 蔡家楣（杭州浙江工业大学软件开发环境重点实验室 310014）

摘 要：本文提出了一个适应多种移动终端技术的无线安全中间件的设计方案，介绍了中间件的各部分内容、实现并将此中间件应用于无线电子商务中，具有一定的实践意义。

关键词：中间件 无线安全 无线电子商务 密码服务 J2ME

1 引言

随着无线网络和信息化技术的进步，移动电子商务得到了迅猛的发展。目前，在安全应用框架上，主要采用了无线公钥基础设施（WPKI）[1]。

无线公钥基础设施主要由PKI入口、无线网关、CA中心和内容服务器等部分组成。移动终端利用WTLS层与无线应用协议网关建立安全连接，通过WAP网关使用SSL与Internet网络中的内容服务器进行安全通信。构建这样的一个WPKI是一个复杂的过程，不仅需要底层加密算法库的支持，而且还需维护一个无线证书认证中心。目前许多国际厂商采用了较X509证书更小巧的WTLS证书以及ECC公开密钥加密系统来优化WPKI，但是运行整个WPKI系统本身就将耗费大量时间与运算资源。

从加密技术上看，在一般嵌入式操作系统上也可实现信息加密与解密、信息摘要、单向散列、数字签名、密钥生成与存储等功能，现有的很多解决方案主要采用动态口令加密认证和数据信息摘要加密通信，加密接口捆绑在操作系统级，一般没有证书处理的功能，这样虽然可快速地提供安全服务，但安全级别受限，并且应用不够灵活。

随着无线通信技术的发展，基于K-Java技术和Brew等新技术的移动终端可直接通过HTTP协议接入Web应用服务器。虽然这些技术使得移动终端具备了一定的独立编程能力，但是安全技术的实现依然受限于终端计算资源。

因此，为了适应无线多终端的处理能力，本文提出了一套既满足高强度安全需求又适应无线设备运算环境的安全解决方案，并将此方案应用于基于无线J2ME技术无线电子商务中，取得了良好的实际效果。

2 安全中间件的设计与实现

2.1 安全中间件的模块设计

本文提出了无线安全中间件主要采用简化的PKI框架，同时兼顾无线通信的特点，利用中间件概念，完成对PKI基本功能（如加密解密、信息摘要、单向散列、数字签名、签名验证、证书认证以及证书和密钥生成、存储、销毁等实现与封装扩充），形成一致的系统安全服务接口和通信安全服务接口。该中间件屏蔽了安全技术的复杂性，向用户提供统一的安全接口标准，满足各种级别的安全需求应用，能与其他无线应用中间件一起无缝地整合于无线应用平台。

系统采用分层结构，如图1所示：

2.1.1 密码服务

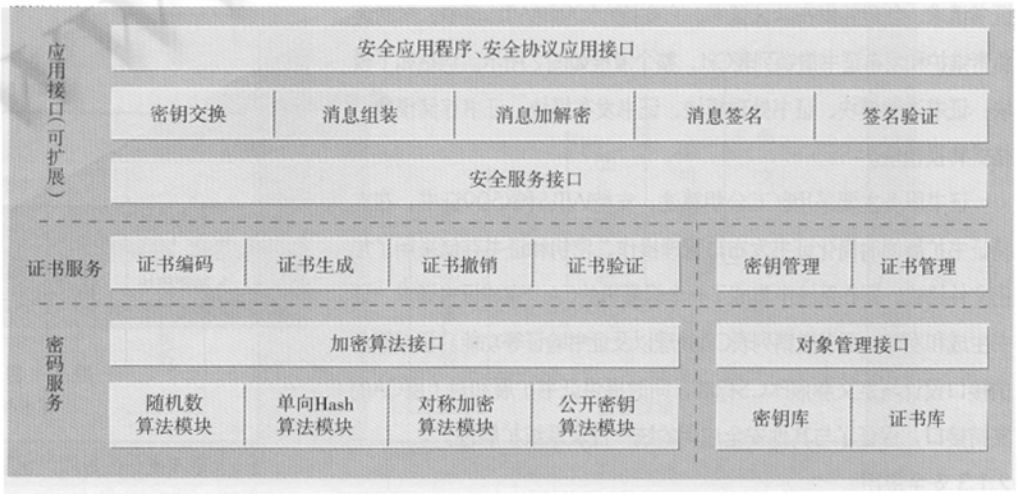

图 1 模块结构图

密码服务是整个中间件的核心，在功能上完成基于密码学的各类安全应用，如数据加密、解密、哈希生成、数字签名及验证等，它是证书应用及上层所有应用程序或安全协议应用的基础，同时所提供的统一密码服务接口能满足个性化的安全服务需求。密码服务的底层模块组成一个加密库，安全服务接口及之上的密钥交换等实现都构建在此加密库基础上。由以下各部分组成：

（1）随机数模块：采用伪随机数序列设计，支持RC4、SEAL和YARROW[3]算法增强伪随机数发生器的安全性。同时针对PKCS#11和CryptAPI，在接口设计上考虑了对第三方密码服务的支持。密钥生成的安全性关键就取决于随机数发生器的设计。

（2）Hash模块：包含MD4、MD5、SHA等算法，提高了应用中Hash运算的正确性和安全性。哈希算法是数据完整性的安全保障，主要完成单向哈希功能。

（3）对称加密模块：提供高强度的分组加密算法，且支持各种加密模式，主要用来加密传输的信息。密钥长度的选择兼顾算法安全与执行速度。

（4）公钥模块：提供Diffie-Hellman、RSA和ECC三种可选的系统。公开密钥算法是安全认证、数字签名及证书应用的基础，而ECC算法是计算资源有限的移动终端的首选，在大数处理时应用中国余数定理来优化设计，签名方案采用ElGamal算法。

加密库设计采用了统一的算法结构定义，具备良好的扩展性和通用性，算法信息的通用数据结构定义如下：

密钥管理时根据密钥类型统一定义钥匙串存放各类密钥，在算法功能实现上，上述的几个方面在逻辑上独立构成算法库，下面概要地介绍几个算法库的功能实现及特点。

2.1.2 证书服务

证书服务即一个简化的CA（证书认证中心），遵循国际标准接受证书请求、创建并发布认证证书，它支持X.509和WTLS证书，同时还负责维护和发布证书撤销列表CRL，整个流程如图2所示。包括如下模块：证书注册模块、证书处理模块、证书发布模块、证书存储模块、格式转换模块。

证书服务主要采用ECC公钥算法，支持WTLS和X509证书，在支持证书扩展同时简化证书发布与管理操作，密钥和证书存储采用了加密文件格式，即在系统中集成了一个轻量级的CA，完成证书请求、证书生成和发布、证书撤销列表CRL处理以及证书验证等功能。证书服务的接口设计与定义参照PKCS标准，同时提供证书扩展和对上层CA的支持接口，保证了与其他安全应用的统一性及系统扩展性。

2.1.3 安全应用

安全应用是对上述两大模块的封装，包括采用Diffie-Hellman协议实现密钥交换接口设计，利用证书编码、证书验证和加密算法接口实现安全消息处理函数，如验证摘要信息、验证消息签名、消息签名并加密，以及解密消息并验证数字签名等，提供了不同安全级别应用的简易操作接口。

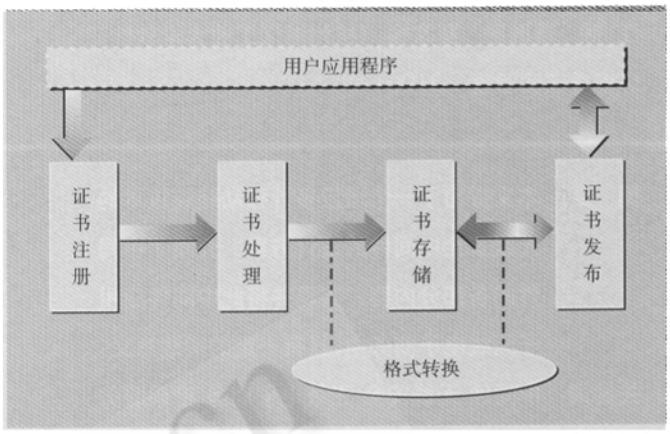

图2 证书服务流程图

综上所述，底层是提供证书服务和密码服务的两大主要功能模块，两者之间有相互调用的接口；安全服务层真正执行证书操作和密码操作，提供安全服务接口；安全应用层则提供安全等级服务操作，同时为无线应用提供接口服务。通过在各层封装安全API以向各种系统环境提供统一的安全操作接口并且各层同时向其他应用程序提供对外接口。

2.2 密码函数的实现

整个密码服务是安全中间件的核心部件，系统流程如图3所示，它的核心主要包括两个提供安全操作的加密函数库：基本密码函数库和高级密码操作函数库。

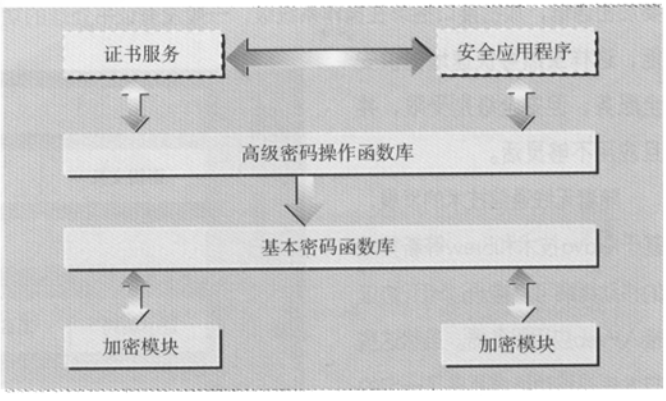

图3 密码服务流程

（1）基本密码函数库。包括一些基本的有关密码操作的加解密函数、信息摘要函数、数字签名函数等（表1示例了部分函数说明）。

鉴于通用性的考虑，真正执行这些基本密码函数的代码由图中最下层的密码模块实现，这可用捆绑在操作系统级的进程设计实现，函数接口统一定义并符合PKCS#11标准。每个密码模块可独立实现各类密码算法，算法相关的数据结构统一定义，例如下面给出一个算法信息的数据结构：

```
typedef struct CryptoAlgInfo{
        long status;        /*算法状态*/
        long type;          /*算法类型*/
        char *name;         /*算法名称*/
        long id;            /*算法标识符*/
        long version;       /*算法版本号*/
        long flags;         /*算法实现途径类型（如多线程）*/
        long maxcontexts;   /*算法支持的最大处理字节数*/
        long blocklen;      /*该算法执行时输入所需的长度*/
        long keylen;        /*该算法执行时使用的钥匙长度*/
        long outlen;        /*该算法执行时输出所需的长度*/};
```

表1 部分基本密码函数

基本函数	函数说明
CryptEncrypt	加密数据函数
CryptDecrypt	CryptoEncrypt加密的解密函数
CryptGenKey	随机数产生函数
CryptSignHash	数据哈希签名
CryptVerifySignature	签名验证

（2）高级密码操作库。主要是封装基本密码函数和证书服务函数的函数，向上给应用程序提供简单易用的安全函数接口，主要包括消息函数、签名认证函数、证书编解码函数以及证书管理函数等（表2示例了部分函数说明），其中前两者可用于对敏感信息进行加密或签名

表2 部分高级密码函数

高级函数	函数说明
CryptVerifyMessageDigest	验证消息摘要
CryptVerifyMessageSignature	验证消息签名
CryptSignAndEncryptMessage	消息签名并加密
CryptDecryptAndVerifyMessag eSignature	解密消息并验证数字签名（需证书服务函数支持）

处理，可保证网络传输的私有性；后两者通过对证书的使用保证网络信息交流中的安全性。当然，向下需基本密码函数接口以及上述证书服务函数接口的支持。

3 无线安全中间件的应用

为保证网上交易的安全，通常需要考虑以下四个基本要素：身份认证、信息一致性、交易不可抵赖性、信息保密性。这些要素在无线电子商务中特别是在线交易中的安全性问题表现尤为重要。

J2ME 应用程序可以在 HTTP 协议上使用 XML 数据格式与后端服务器和其他 J2ME 应用程序通信。由于目前K-Java手机在运算速度和程序容量方面的功能有限性，用Java做出的解决方案还不够完整，可以考虑在在线交易时利用本文提出的轻量级的无线加密包通过XML 解析器实现xml数字签名。现有的XML 数字签名协议可以定义如何对 XML 文档的部分或全部进行数字签名以保证数据完整性，XML 密钥管理规范（XML Key Management Specification (XKMS)）格式封装与 XML 数字签名一起分发的公钥。

以下是J2ME手机验证服务器的过程。

其执行步骤如下所示：

（1）服务器提供要签名的明文信息；

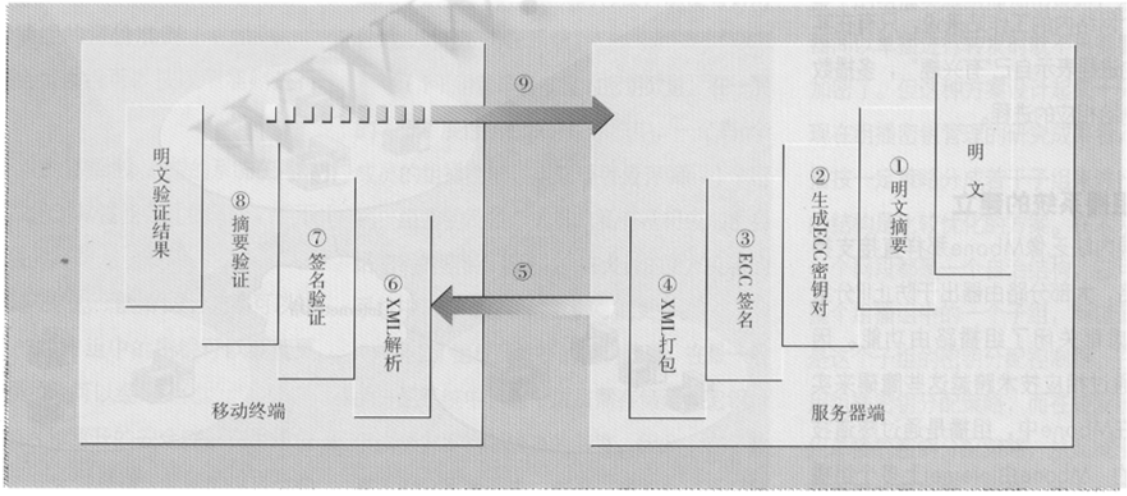

图 4 手机端验证服务器 XML 签名

下转第 46 页 >>

上接第31页

（2）服务器调用安全中间件利用Hash模块生成数据摘要；

（3）服务器调用安全中间件利用公开密要算法模块和随机数模块生成ECC算法密钥；

（4）调用安全服务接口实现对数据的ECC签名；

（5）利用xml安全协议生成XML数据包；

（6）通过TCP/IP协议将经过xml签名的数据包传递给移动终端；

（7、8）移动终端利用安全API接口实现执行与上述相反的过程实现签名的验证过程；

（9）将验证结果返回给服务器。

经过实验表明在j2me等受限环境下，使用椭圆曲线加密算法比rsa要更适合应用于无线环境。目前实现椭圆曲线加密算法的常用方法有：基于素数模（一些免费的第三方加密包例如bouncycastle包里就采用这种实现机制）和基于最佳正交基以及基于不可约多项式方法。

本文在实际使用时采用了基于最佳正交基的椭圆曲线加密算法。

当椭圆曲线的密钥长度为174位的时候，它的性能比密钥长度为1024的rsa算法性能要高，速度比rsa要快20多倍。把密钥降到120位的时候，它的签名算法的时间开销一分钟都不到（处理机频率为16兆），它的安全性能比512位的rsa要高，能满足行业交易的需要。

4 结束语

本文提出的无线安全中间件以各种集成API的形式实现对外提供各种安全服务需要，具有较好的平台无关性和功能扩展性，在实现上能充分考虑无线环境的限制条件，具有简单、灵活等特点可直接应用于各种PDA，对具有Java,Brew技术的等计算能力较低的移动终端可以将上述功能经配置后进一步简化处理流程，可以容易的实现与第三方开发包配合使用。实验表明，该无线安全中间件能够很好的支持无线安全应用，在无线电子商务的安全领域具有良好的实用价值。

参考文献

1 Wireless Application Protocol Public Key Infrastructure Definition http://www.wapforum.org。

2 Internet X.509 Public Key Infrastructure Certificate and CRL Profile[S]. RFC2459,1999.9。

3 Public-Keys Cryptography Standards[S]. RSA Laboratory, 1993-2001。

4 J.Kelsey,B. Schneier. The YARROW-160 PRNG [OB], http://www.counterpane.com/ yarrow-presentation.pdf。

5 朱斌，、张琳峰、朱海云，基于证书的移动通信认证模型[J]，电子学报,2002,30(6):868-871。

6 韩智勇、范平志、郑彩花，证书编解码及其实现方法[J]，计算机应用,2002,22(2):43-45。

7 Bruce Schneier著,吴世忠等译,应用密码学[M]，机械工业出版社,2000.1。