

一种移动 Web 服务安全性技术方案

邢翠芳,李 瑛,赵海冰,杜 晶

(海军航空工程学院 基础部,山东 烟台 264000)

摘 要:为解决移动 Web 服务的安全性问题,文中首先着重研究了适用于 Java ME 平台的相关加密、摘要和数字签名算法,同时将这些算法应用于移动设备模拟器上以验证其性能,通过分析比较模拟器上的测试数据,从而提出一种适用于移动 Web 服务的安全性技术方案。最后,通过一个移动机票预订系统来验证技术方案的可行性,该系统能充分考虑端到端安全架构的要求。在安全性上,也基本实现了安全性所要求的目标。

关键词:移动 Web 服务;安全;加密;数字签名

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2013)04-0122-04

doi:10.3969/j.issn.1673-629X.2013.04.030

A Mobile Web Service Security Technology Scheme

XING Cui-fang, LI Ying, ZHAO Hai-bing, DU Jing

(Department of Basic Sciences, Naval Aeronautical and Astronautical University, Yantai 264000, China)

Abstract: In order to solve the security problem of mobile Web service, firstly studied the encryption, digest and digital signature algorithms which applied for the Java ME platform and the performance of these algorithms were tested on mobile device emulator. Through analysis and comparison of test data in emulator, a mobile Web service security technology scheme was proposed. To test the safety and the feasibility of the scheme, designed and constructed a mobile air ticket booking system. The system considered fully the end-to-end security requirement, which basically achieved the safety needs.

Key words: mobile Web services; security; encryption; digital signature

0 引 言

如今移动设备和网络的发展使得移动商务成为可能,移动设备通过 Web 服务的方式让人们实现购物支付、银行交易等业务。随着应用的不断升级,移动 Web 服务将逐渐发展成为 Web 服务领域的一种重要访问方式^[1]。

基于 Java 的移动 Web 服务在移动电子商务的应用中有很好的发展,但是安全性仍是亟待解决的问题之一。由于无线信号在传输过程中经常会被劫持和监视并且用户使用的手持设备存在内存空间小和运算能力有限等特点^[2],使得移动客户端成为移动 Web 服务中最薄弱的环节。另一方面,目前 SSL/TLS 安全协议虽然在电子商务领域得到普遍应用,但是它不能很好地适用于 Web 服务领域^[3],它所提供的服务仅限于点对点,不具备在整个应用程序范围内实现端到端的安全能力,当信息要传送给多个用户时,SSL 并不能起到

作用。因此,安全性问题是一个限制移动 Web 服务突破性发展的瓶颈。下面就针对移动 Web 服务在使用过程中出现的安全问题提出一种解决方案。

1 移动平台上的安全技术分析

在移动 Web 服务开发中 Java 平台起着很重要的作用^[4]。由于 Java EE 平台能对 Web 服务提供良好的技术支持,所以在 Web 服务端得到了广泛应用。而 Java ME 平台能够很好地满足电子消费和嵌入式设备开发的需要,为所有无线设备提供了跨设备的兼容性、高级语言功能和大量库^[5],其主要应用在移动客户端,目前,最常用的适用于 Java ME 平台的加密包是 Bouncy Castle。Bouncy Castle API 是一种用于 Java 平台的开放源码的轻量级密码术包,它包括一个支持 J2ME 的版本,并支持大量的密码术算法,同时还提供 JCE 的实现^[6]。

1.1 加密算法

加密算法通常分为两大类:“对称式”和“非对称式”^[7]。对称加密算法又分为块式加密算法和流式加密算法。流式对称加密算法的应用相对较少,这里不

收稿日期:2012-07-26;修回日期:2012-10-27

基金项目:航空科学基金(20110184)

作者简介:邢翠芳(1982-),女,山东威海人,硕士研究生,研究方向为计算机网络与安全。

做研究。常见的块式加密算法有 DES、IDEA、AES 和 Blowfish,非对称加密算法的例子主要有:RSA、Elgama 和 ECC 等。

1.1.1 对称加密算法

Bouncy Castle API 包中包含 DESEngine、DESedeEngine、IDEAEngine、AESEngine 等密码引擎用来提供对 DES、三重 DES、IDEA、AES 等块式对称加密算法的支持。由于 DES 的密钥太短,影响保密强度,当前采用的 DES 算法一般是 DES 的强化组合模式三重 DES 算法。下面在 Java Wireless Toolkit 2.5.2(以下简称 JWT)平台模拟器上对三重 DES、IDEA、AES 三种常用的对称加密算法进行测试。

固定密钥长度,将 VM 速度由 1000b/ms 降低至 359b/ms,此时,AES 算法生成密钥的时间从原来的 0 增至 65ms,稍有增加,加解密的时间仍为 0;三重 DES 生成密钥的时间不变,但加解密时间从原来的 66ms 增至 209ms;IDEA 加解密和生成密钥的时间均仍为 0。当 VM 速度保持 1000b/ms 不变时,AES 和 IDEA 生成密钥、加解密的时间均为 0,三重 DES 的加解密时间为 66ms;增加密钥长度,AES 生成密钥的时间有所增加,但加解密的时间不发生变化。

可见在移动设备模拟器上 AES、三重 DES 以及 IDEA 三种算法的加解密时间都非常短,都能够保持在 1s 之内,而在性能方面,三重 DES 算法要明显弱于 AES 和 IDEA 算法。而 IDEA 算法由于受专利保护使用起来不太方便,本方案将选择 128bit 的 AES 算法作为对称加密算法。

1.1.2 非对称加密算法

Bouncy Castle 包中包括 RSAEngine 和 ElGamaEngine 密码引擎,同时提供 RSA 和 ElGamal 两种非对称加密算法的实现。由于非对称加密算法的加密和签名过程互为逆过程,因此将在后面讨论签名算法的同时对其性能一起分析。

1.2 摘要算法

摘要算法主要包括 MD5(Message Digest Algorithm 5)和 SHA(Secure Hash Algorithm)。SHA 家族有五个算法,分别是 SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512。后四种常被称为 SHA-2。而 SHA-1 在很多安全协定中广泛应用,曾被视为是 MD5 的后继者。Bouncy Castle API 主要提供了两种摘要算法:MD5 和 SHA-1。

将两种算法在 JWT 模拟器上进行测试,结果表明生成摘要的效率非常高,消耗时间都很短。但现在很多加密包中不再提供对 MD5 的支持。而 SHA-1 生成摘要长度为 160bit,比 MD5 长,其安全性也高。所以文中的技术方案将采用 SHA-1 摘要算法。

1.3 数字签名算法

数字签名是在一端生成密钥和签名,在另一端验证签名^[8]。常用的数字签名算法有 DSA(Digital Signature Algorithm)、RSA 和 ECDSA 三种^[9]。Bouncy Castle 包提供了 DSA、RSA、ECDSA 三种算法的 Java 实现。由于签名过程都选用 SHA-1 作为摘要算法,所以产生摘要的时间完全相同,这里就只需要测试一下生成密钥、生成签名以及验证签名所耗时间。测试过程中,首先设定 DSA/RSA 的密钥长度为 1024bit,ECC 的密钥长度设为 160bit,然后用不同的 VM 速度模拟不同性能的设备。测试结果如表 1 所示。

表 1 不同速度设备上的算法性能			
VM 速度(b/ms)		1000	350
生成密钥时间(s)	DSA	5798.832	17596.745
	RSA	1212.678	3789.642
	ECDSA	83.554	359.123
生成签名时间(s)	DSA	14.187	44.352
	RSA	24.785	75.347
	ECDSA	90.898	378.268
验证签名时间(s)	DSA	32.892	99.951
	RSA	1.890	5.132
	ECDSA	107.450	476.912

数据显示,当 VM 速度由 1000b/ms 变为 350b/ms 时,密钥和签名的生成以及签名的验证时间增幅都很大,后者基本能够达到前者的 3 倍。由此可见,当固定签名算法的密钥长度时,签名操作的效率将直接取决于移动设备的性能。

将 VM 速度恢复至最大值 1000b/ms,再测试不同密钥长度下,三种算法在移动设备上的性能,结果如表 2 所示。

表 2 不同密钥长度的算法性能				
密钥长度(bit)		768/132	1024/160	2048/192
生成密钥时间(s)	DSA	3299.535	5823.833	53267.125
	RSA	601.766	1254.755	32353.765
	ECDSA	68.857	84.492	129.475
生成签名时间(s)	DSA	9.684	15.021	61.429
	RSA	12.012	25.309	207.181
	ECDSA	70.691	91.671	127.102
验证签名时间(s)	DSA	19.822	33.598	136.976
	RSA	1.142	1.915	7.021
	ECDSA	91.683	114.122	168.631

实验数据表明等长密钥且等安全强度的情况下,在生成签名时间方面,DSA 最长,而 ECDSA 最短,且最长与最短时间相差悬殊;增加密钥长度后,DSA 和 RSA 涨幅非常大,而 ECDSA 则相对平缓。生成签名时间方面,三者总体差别不大,增加密钥长度后,同样是 DSA 和 RSA 的涨幅要大于 ECDSA。验证签名时,RSA 所需时间最短,且增加密钥长度后,其增幅也相对较小。

综上所述,本方案将采用 ECDSA 算法在移动端产生密钥,用 RSA 算法在客户端验证签名,若在移动客

户端已经拥有私钥,那么也选择 RSA 算法进行数字签名。

2 移动 Web 服务安全性技术方案的实现

下面将设计一个移动机票预订服务系统以验证上述方案的可行性。在实现的过程中,将第三方的安全工具包 Bouncy Castle 引入其中。

2.1 系统架构

移动机票预订服务系统是一个能够应用于移动终端设备(手机、PDA 等)的系统。系统包括移动客户端、服务提供端和数据库三部分。使用 Java ME 作为移动客户端开发平台,采用 Java EE 平台来构建服务端的 Web 服务,采用 SQL SERVER 作为数据库,而服务器则采用 Sun 公司最新开发的 GlassFish V2。

2.1.1 系统功能

系统主要包含移动天气预报服务和移动机票预定服务两大功能模块。每一部分的具体功能如图 1 所示。

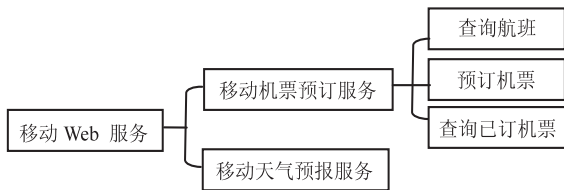


图 1 系统功能结构图

移动天气预报服务模块主要提供中国各大机场所在城市近一周的天气情况。该模块是为了满足客户在查询机票时了解当地天气的需求。天气预报信息对用户来讲是公开、不涉密的,因此设计该模块时在安全方面无需做太多考虑。

移动机票预订服务模块包括查询航班、预订机票和查询已定机票三种功能。系统充分考虑端到端的安全方案,客户端进行访问之前,需要在服务端创建和发布服务。本系统在机票预订模块完成网上支付功能时,借助于模拟的银行支付网关来实现。

2.1.2 系统的安全架构

系统的安全架构如图 2 所示。在 Java EE 服务端和 Java ME 客户端各有一个密钥库文件,该文件需事前生成并存储在相应位置,其作用是提供用于加密的

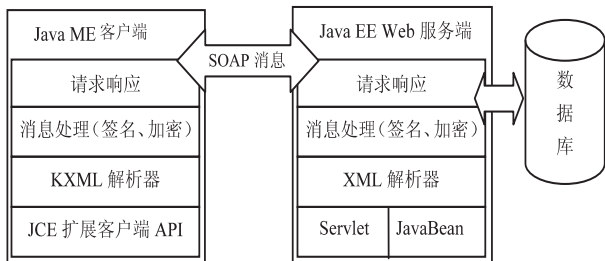


图 2 系统安全结构图

私钥和用来向接收方证明其身份信息的数字证书,采用 XML 加密和签名技术保证消息传输过程的安全性,需要使用的安全算法由 Bouncy Castle 来提供。

2.2 安全性实现

利用 NetBeans 6.5 和 GlassFish V2 服务器来创建和部署系统的服务端。在客户端,Java ME 访问远端的 Web Service 时,利用第三方的工具包 kSOAP^[10]。

2.2.1 JCE 配置

Bouncy Castle JCE Provider 是一个能很好地适用于移动设备领域的安全提供者。Java 应用程序使用 JCE 类之前,首先需要将下载的文件包 Bouncy Castle Crypto 解压缩至 JDK 的 classes 目录下。第二步需要配置安全属性文件 java.security,该文件位于 jre 安装路径下的 lib/security 目录,它定义了当前可以使用的加密提供者。在属性文件中,需要按照如下格式设置加密提供者的优先级:

security.provider.<n>=<masterClassName>,这里的 n 是优先级,其取值为大于 0 的正整数。masterClassName 是加密提供者的主类名称。

例如:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.sun.rsa.jca.Provider
```

表示使用 Sun 和 Provider 两个加密提供者。当需要用到一个加密算法时,虚拟机将根据优先级依次访问加密提供者,寻找需要的算法。在本方案中需要将新的加密提供者 Bouncy Castle Provider 加入进去,在文件中插入代码如下:

```
security.provider.3=org.bouncycastle.jce.provider.
BouncyCastleProvider
```

2.2.2 身份验证机制

在服务端,用 1024bit 的 RSA 算法为移动客户端和服务端分别生成一个数字证书。用于验证客户端的身份和信息的加密的客户端数字证书,在下载客户端应用程序时将会一起下载到客户端。Keytool 是私钥仓库和与之相关的 X.509 证书链的管理工具,它通常将密钥和证书都储存在一个密钥仓库里。使用 Keytool 生成一个 X.509 数字证书用来为服务端进行服务。使用 KeyStore 类生成 .jks 格式的证书文件后,可以在应用中 import 导入、export 导出和 list 显示证书文件。

2.2.3 加密和签名

使用 Bouncy Castle API 提供加密和签名的实现。在移动客户端需要完成以下操作:读取 RSA 私钥;对待发送信息进行数字签名;用 AES 密钥(随机生成)加密签名后的信息;接收服务器端发送过来的对称密钥并用 RSA 公钥加密;加密后重新格式化为 SOAP 的形

式发送给服务端。服务端接收到 SOAP 信息后,需要完成的操作包括:读取 RSA 私钥;解密客户端发送的消息;获取 AES 对称密钥并用其解密消息;获取客户端签名并验证,验证通过则接受请求,否则拒绝服务。系统中 SOAP 消息的签名和加密的过程如图 3 所示。

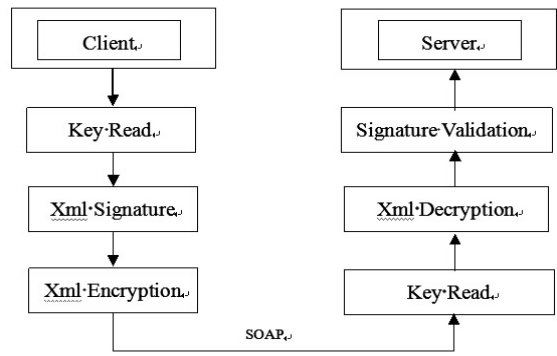


图 3 签名和加密过程

3 结束语

移动电子商务作为目前互联网电子商务不可或缺的一部分,其所扮演的角色和涉及的内容正在不断扩大。为解决当前移动 Web 服务在移动电子商务应用过程中出现的安全性问题,文中通过分析比较几种流行的安全技术,提出一种适用于移动 Web 服务的加密和数字签名方案。该方案将 Java ME 和 Web 服务技术紧密结合,并引入第三方 Bouncy Castle 包创建安全模型。最终该方案在一个移动机票预订系统上进行验

证,基本实现了系统所要求的消息完整性、机密性、真实性和不可抵赖性。

参考文献:

[1] 王 斌,戚银城. 基于 Web 服务的移动电子商务技术研究[J]. 电脑与信息技术,2005(5):8-11.

[2] 孟 伟,张 璟,李军怀,等. Web 服务安全模型研究与实现[J]. 计算机工程与应用,2006(26):134-136.

[3] 张劳模. 基于 J2ME 平台的无线 Web 服务安全性技术应用研究[D]. 成都:成都理工大学,2004.

[4] 李程程,张永胜,李 静,等. 一种简单的 Web 服务安全通信模型研究[J]. 计算机技术与发展,2010,20(9):157-160.

[5] 杨 雄,赵远东. 基于 J2ME 的无线移动商务安全应用研究[J]. 计算机应用与软件,2006(4):110-112.

[6] Xuan Zuguang, Du Zhenjun, Chen Rong. Comparison Research on Digital Signature Algorithms in Mobile Web Services[C]//IEEE Int'l Conf on ISM. [s. l.]:[s. n.],2009:216-224.

[7] 王凤英. 网络与信息安全[M]. 北京:中国铁道工业出版社,2010.

[8] 郭金良. XML 数字签名及加密技术的研究与实现[J]. 科学技术与工程,2008(8):5080-5083.

[9] NIST. Digital Signature Standard[S/OL]. 2008. http://csrc.nist.gov/publications/drafts/fips_186-3/Draft_FIPS-186-3%20November2008.pdf.

[10] Balani N. Deliver Web Services to Mobile Applications[EB/OL]. 2003. <http://www.ibm.com/developerworks/wireless/edu/wi-dw-wiwsvs-i.html>.

(上接第 121 页)

可广泛用于教育培训、商业娱乐、医疗、考古挖掘、机器人等领域。

参考文献:

[1] Dalal N, Triggs B. Histograms of Oriented Gradients for Human Detection[C]//Proceedings of CVPR. Los Alamitos, CA, United States:IEEE,2005:886-893.

[2] 黄文丽,范 勇,李绘卓,等. 基于区域纹理的运动目标检测方法[J]. 计算机应用研究,2011,28(5):1968-1971.

[3] Biswas K K, Kumar B S. Gesture Recognition Using Microsoft Kinect[C]//Proceedings of the 5th International Conference on Automation, Robotics and Application. Los Alamitos, CA, United States:IEEE,2011:100-103.

[4] Ridler T W, Calvard S. Picture Thresholding Using an Iterative Selection Method[J]. IEEE Trans. on System, Man and Cybernetics,1978,8(8):630-632.

[5] 侯艳丽. 基于模糊隶属度的并行彩色图像分割[J]. 计算机技术与发展,2011,21(8):109-111.

[6] 林洪文,涂 丹,李国辉. 基于统计背景模型的运动目标检测方法[J]. 计算机工程,2003,29(16):97-99.

[7] 徐正光,鲍东来,张利欣. 基于递归的二值图像连通域像素标记算法[J]. 计算机工程,2006,32(24):186-188.

[8] 高若云,江 灏,刘瞰东. 基于方向梯度的相关图算法在人体动作识别中的应用[J]. 电脑知识与技术,2010,6(7):1686-1688.

[9] 王 亮,谭铁牛,胡卫明. 人运动的视觉分析综述[J]. 计算机学报,2002(3):225-237.

[10] Rui Y, Anandam P. Segmenting Visual Actions Based on Spatiotemporal Motion Patterns[C]//Proceedings of IEEE Conference on Computer Vision and Pattern Recognition. Los Alamitos, CA, United States:IEEE,2000:111-118.

[11] Ali A, Aggarwal J K. Segmentation and Recognition of Continuous Human Activity[C]//Proceedings of IEEE Workshop on Detection and Recognition of Events in Video. Los Alamitos, CA, United States:IEEE,2001:28-35.

[12] Ikemura S, Fujiyoshi H. Real-time Human Detection Using Relational Depth Similarity Features[C]//ACCV 2010, Lecture Notes in Computer Science. Los Alamitos, CA, United States:IEEE,2011:25-38.

一种移动Web服务安全性技术方案

作者: [邢翠芳](#), [李瑛](#), [赵海冰](#), [杜晶](#)
作者单位: [海军航空工程学院 基础部, 山东 烟台264000](#)
刊名: [计算机技术与发展](#)
英文刊名: [Computer Technology and Development](#)
年, 卷(期): 2013(4)

本文链接: http://d.g.wanfangdata.com.cn/Periodical_wjfz201304032.aspx