移动电子商务安全问题研究

徐洪峰[1],徐 曦[2],曾 杰[3]
(1.贵州师范大学 经济与管理学院,贵州 贵阳 550001;
2.湖南科技大学 信息与电气工程学院,湖南 湘潭 411100;
3.中国人民银行 贵州省中心支行,贵州 贵阳 550001)

摘 要:无线网络的开放性和网络体系结构的不安全性,使得移动电子商务比电子商务存在更多的不安全因素,如网络中信息窃取、信息篡改、认证身份假冒等。为了解决移动电子商务交易和网络数据传输中的潜在威胁,采用移动网络来改进TCP/IP网络体系的安全,同时采用WAP协议框架中的安全传输协议、安全网关和安全层次以及加强数据传输过程中的加密和认证算法,解决了交易传输中的明文数据和用户攻击。改进移动电子商务数据的安全传输,实践证明采用上述方法能有效改进移动电子商务中的安全隐患。

关键词:移动电子商务;WAP;加密;认证
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)11-0236-03

Research of Mobile E-Commerce Safety Problem

XU Hong-feng[1],XU Xi[2],ZENG Jie[3]
(1. School of Economy and Management,Guizhou Normal University,Guiyang 550001,China;
2. School of Inf. and Electrical Eng.,Hunan Univ. of Sci. and Techn., Xiangtan 411100,China;
3. Guiyang Central Sub-branch, The People's Bank of China,Guiyang 550001,China)

Abstract:Wireless network openness and network architecture causes the mobile e-commerce to face unsafe factors more than e-commerce,such as the communication content to be easily intercepted,information changed,the correspondence both sides status to be possibly pretended and so on. In order to solve unsteady factors of business in e-commerce and transmission message,use network to improve the safe of TCP/IP network architecture,at the same time using the safe transport protocol,safe gateway and the security level in the WAP protocol framework,as well as the algorithm strengthens the encryption and the authentication in the data transmission,can solve plaintext in transmission business and attack by users. Improving the security of mobile e-commerce data transfer,the result proves those method can improve security of problem in m-commerce.

Key words:m-commerce;WAP;encryption;authentication

0 引 言

移动电子商务(M-commerce)是一种特殊的电子商务体系,它是指用户通过各种移动通信设备,例如手机、个人数字助理、笔记本电脑等,而后通过移动通信网络来进行电子商务交易[1]。移动电子商务将传统的商务和电子商务整合起来,将各种业务流程从有线向无线转移和完善,是电子商务发展的新形态[2]。但由于移动电子商务采用的是无线信道,同时互联网系统结构原有存在的不安全因素,使得在移动电子商务交易过程中存在大量的安全隐患。

收稿日期:2011-04-11;**修回日期**:2011-07-16
基金项目:贵州省教育厅自然基金课题(黔科教20090037)
作者简介:徐洪峰(1977-),男,江西上饶人,硕士,副教授,研究方向为计算机网络、企业信息化、数据挖掘。

1 移动电子商务安全框架体系

移动电子商务的安全体系结构由五个部分组成:移动承载层、加密技术层、安全认证层、安全协议层、应用系统层。安全体系结构图如图1所示,这由上至下的五个部分中的每一层是其上层的物质基础,为其上层提供服务和技术支持;而每层也都是其下层不同应用的扩展。这五部分之间是相互依赖、相互关联的,它们形成一个统一整体,这就是移动电子商务的安全体

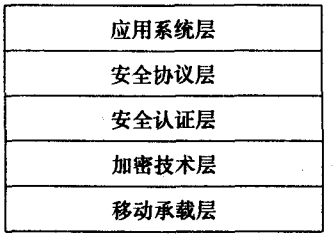

图1 移动电子商务安全体系结构

系结构[3]。

2 存在问题

移动电子商务主要面临着两个方面的威胁:移动通信系统、移动设备自身隐患和 Internet 的安全风险。这些威胁和风险主要包括终端窃取与假冒、无线链路威胁、拒绝服务和交易抵赖、移动设备的隐患等。

2.1 移动通讯系统威胁

①无线链路威胁。由于移动电子商务的特点同时移动通讯的短消息数据大都采用明文传输,这使得通过无线设备进行信息窃听变得简单和容易。在移动电子商务通信过程中是使用无线信道来传输通话内容、用户身份、用户通讯位置、数据信息等,而其他人可以通过适当无线终端设备来窃听在无线信道上传输的上述信息,并且这种方式很难被发现[4]。

②交易抵赖。在电子商务的交易过程中双方都参与了相应的交易过程,但很可能会出现一方否认参与交易,这其中同时可能存在着两种抵赖情形:一种情形是当客户在收到商品之后进行抵赖,不承认收到商品而拒绝支付货款;另一种情形是商家收到货款后进行抵赖,否认已收到货款并且拒绝交付商品。

③假冒攻击。由于无线网络信号的漫游性,攻击者可以利用无线接收设备对无线网络中传送的信息进行截取和窃听,而后通过分析截取到的这些信息来得到用户的合法信息,攻击者就可以利用这个合法信息来进行攻击和欺骗[5]。

④拒绝服务。攻击者的拒绝服务攻击是指攻击者通过对服务主机或者是通信网络进行干扰,使用户数据没有办法及时传递。此外,攻击者还可以通过大量重复发送假冒网络信息单元,这样就可以阻塞合法用户的业务数据、信令信息或控制数据等,从而其他用户就无法接受正常的网络服务。

2.2 移动设备自身隐患

移动设备自身隐患主要包括:移动设备数据自身的安全性、移动设备硬件的弱处理性和移动设备通讯安全性等。

①移动设备数据安全性。

移动通信终端的硬件资源的处理能力低、内存的容量小、数据传输速率由于受地理位置等的限制速度较慢,使得在现在的条件和环境下开展移动支付和交易业务存在更大的限制和隐患。因此,提高移动通讯终端存储能力和处理能力将有助于处理交易数据和移动电子商务的开展,但由于移动终端自身的特点,病毒传染也更加容易。这就意味着容易泄露敏感的企业或个人数据,这使得攻击者可以通过所获取来的移动终端上的数据资源如数字证书、机密数据等,非授权访问企业内部网络的系统资源,或破坏移动通信终端中的数据完整性,从而造成企业或个人的损失[6]。

②移动设备硬件弱点。

如果采用手机实现移动电子商务交易,手机中的重要信息都是存储在 SIM 卡中,因此 SIM 卡是标识移动终端用户的一个重要设备。一旦手机产生丢失,则他人可以复制 SIM 卡中的这些重要信息来进行攻击和欺骗。如果在电子商务交易中使用移动设备来进行用户鉴权,那么 SIM 丢失后非法窃取者还有可能伪装成真正用户参与到电子商务的活动中来。另外,移动设备需要依靠电池来进行工作,如果移动设备持续传输大量数据将会导致网络带宽饱和及设备电池耗尽,从而设备性能降低或掉电停用。这些都是移动设备需要考虑的问题。

③移动设备通讯安全。

移动设备,操作系统,组网技术的多样性、不成熟性及客户群规模加剧了病毒和恶意代码攻击的威胁与风险。无线设备上的口令简单、易攻击性为非法访问应用和数据创造了机会[7]。非法用户可以通过在移动设备上的蓝牙接口来接入它周边的设备,然后通过"网关"利用现有连接进入专用/内联网。入侵者还可以通过射频扫描设备对公共射频进行扫描,从而捕获其中传输的数据,然后利用加密算法中的弱点来解密数据,这样就导致用户信息的泄露。此外,移动电子商务提供了基于位置的服务,但由于移动设备通讯安全性的问题它同时也为用户带来了私密性泄漏问题。

此外,如法律规范不完善,信用意识淡薄、原有 Internet 网络自身存在的不确定的安全隐患、移动设备终端(特别是智能手机终端现在的手机病毒等)和无线网络本身的开放性降低了安全性等原因导致移动电子商务应用过程中存在诸多安全威胁[8]。

3 引起的主要原因

①移动终端限制了安全性能的提高。移动电子商务的交易终端绝大部分都不具备处理高加密信息能力,因此在考虑信息加密过程中,加密算法相对简单,加密强度都达不到安全的程度,无法保证安全交易,同时有线网络环境下运行的安全协议也没有办法在无线环境下运行,所以安全交易机制难以在移动网络环境中运行。

②无线网络本身的开放性降低了安全性。Internet 在最初的设计过程中,没有考虑网络终端之间互联的安全,其安全性存在较大隐患;再加上无线网络传输媒体的开放性以及移动设备存储资源和计算资源的有限性,使得在无线网络环境下,许多有线网络中潜在的安全威胁更加明显,攻击更容易实现。任何用户都可以

借助移动接收设备很容易地接收移动处理的无线信号，利用相应破解软件可以更快速进行信息的破解和还原。

4 解决方案

4.1 WAP 协议框架

考虑到上述的安全性问题及威胁，可以采用 WAP 体系框架来改进数据传输和交易过程中的安全性，通过建立 WAP 网关的 Web 服务器来解决端到端的问题。WAP 的安全机制主要包括 WTLS 协议（Wireless Transport Layer Security）、WAP 身份模块 WIM（WAP Identify Module）、WML 脚本加密接口 WMLSCrypt（WML Script Crypto API）和 WPKI（Wireless PKI）[9]。这四种安全机制可以实现移动电子商务所需的数据保密性、数据完整性、交易方的认证与授权和不可抵赖性四个方面的信息安全特征，如图 2 所示。

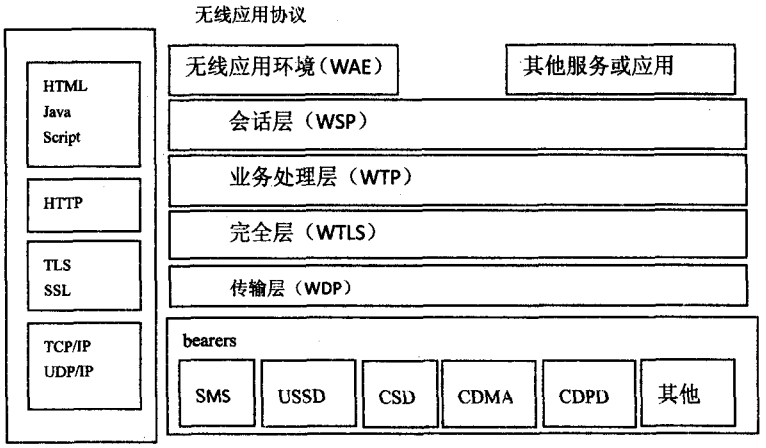

图 2 WAP 体系结构

WAP 的安全会话模式由三个部分组成，一般说来安全的 WAP 会话主要由两部分来完成：第一阶段，网关与服务器间采用安全套接层协议实现数据通信，以保证数据在传输过程的安全性、完整性和数字认证；第二阶段，网关与移动终端之间采用无线传输层安全协议实现通信。在会话过程中首先要实现两个阶段中不同格式之间的转换，实现有效传输；再将转换后的数据传输给手机用户；从手机发往 Web 服务器的消息同样经由网关将 WTLS 格式转换成 SSL 格式。在安全会话过程中网关最主要的功能就是实现两个协议数据格式转换的功能。考虑到 SSL 协议要求高处理能力和一个相对高带宽、低延迟的 Internet 连接，这是手机所不具备的。因此通过简化 WTLS 协议便于手机终端能实现信息的安全处理，确保了手机用户能够通过 Internet 进行安通。

为了解决 WAP 服务器配置过程中费用过高问题和 WTLS 与 SSL 会话通过存在的协议数据转换间的明码问题[10,11]，可以考虑在通讯传输的过程中，进行一定的加密，现在用的最多的是椭圆加密 ECC，主要考虑的因素是该加密过程中密钥长度为 163 位，加密能力和程度可以达到 RSA 加密密钥 1024 位的加密程度。同时采用双加密模型来完善移动终端、WAP 网关和内容服务器之间的数据传输安全，如图 3 所示。

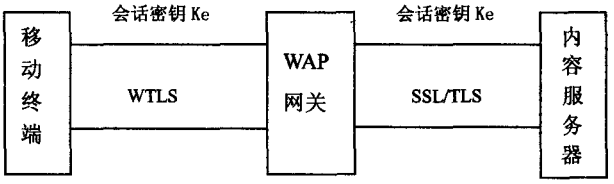

图 3 数据传输转换过程的双重加密过程

4.2 加密和认证手段

①加密技术。当无线网络中传输数据被窃取时，使用现有的加密技术对传输数据进行加密可以有效降低风险。移动通信网中一些加密技术还存在许多缺陷和弱点，对此可以使用更为安全的 IPSEC、WTLS 和 TPKDP 等安全协议。

②严格的用户鉴权。移动电子商务交易过程中的金融交易需要有严格的用户鉴权。现可以使用“双向”鉴权机制，也就是基于客户所拥有的和所知道的事物的鉴权，来确保移动环境下的交易安全性。

③授权。授权解决方案用来管理和集成用户接入控制及授权信息，在必要时也可对用户接入加以限制。授权包括两种方式，即基于功能的授权（定义每位用户进行授权的功能）和基于接入控制表 ACL 的授权（定义用户可以允许进入网络的策略和资源）。简单的授权检查可在无线环境中的各种位置完成。

④WPKI 技术。可通过部署无线公共密钥基础设施（WPKI-Wireless Public Key Infrastructure）技术来实现数据传输路径真正的端到端的安全性、安全的用户鉴权及可信交易[11,12]。WPKI 使用 ECC 椭圆曲线加密算法和压缩的 X.509 数字证书来进行管理，对于证书的公钥管理采用第三方认证中心 CA 进行，能够有效实现用户身份的认证。

5 结束语

考虑到 WAP 存在的缺陷，在相应的认证中心签发数字签名和数字证书的过程前，考虑加入相应的加密过程，保证用户信息的唯一性。但是相应的加密算法要考虑移动通讯设备的处理能力和存储能力，所以可以选用 ECC 加密算法来实现信息的加密。此外，利用

（下转第 242 页）

授信证撤销服务;在服务网(外部)部署劳动保障机构授信证服务系统,提供授信证发布、授信证状态查询、授信证信息查询服务[13]。为保障系统安全性,在劳动保障机构授信证服务系统中部署加密服务器,以提供加解密、签名及签名验证、数字信封服务、产生随机数和对数据进行数字摘要等多种必要的密码服务。

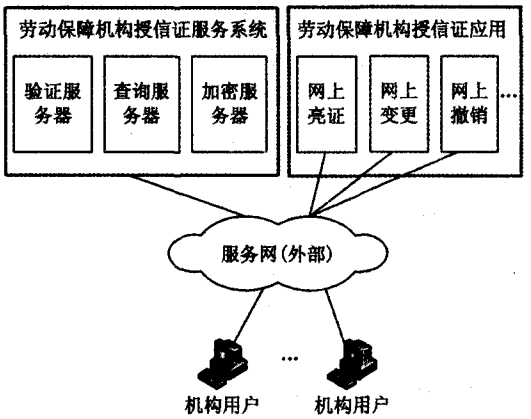

图 4 劳动保障机构授信证应用场景

4 结束语

劳动保障机构授信证颁发与管理体系的研究,加强了劳动保障业务代理机构和中介机构的诚信管理,解决了劳动保障公共服务中的虚假信息、"不法中介"等信任问题,对促进我国劳动保障公共服务的业务代理和中介服务市场的规范化发展,营造完善、安全、诚信、符合我国国情的劳动保障公共服务网络环境,进一步加强劳动保障业务代理机构和中介机构的服务水平和能力做出了积极贡献。

参考文献:

[1] 姜 岚,王宏滨. PKI/CA 技术在电子政务中的应用[J]. 黑龙江科技信息,2010(12):69-69.

[2] 邓晓军. PKI 技术及其应用的分析[J]. 计算机技术与发展,2008,18(6):144-147.

[3] 冉 艳,胡学钢. 构建市级电子政务安全平台[J]. 计算机技术与发展,2007,17(8):144-147.

[4] 中华人民共和国国务院令第 423 号. 劳动保障监察条例[S]. 2004.

[5] 杨 宇. 基于 PKI 身份认证系统的研究与实现[D]. 成都:电子科技大学,2009.

[6] 宁红宙,华 刚,金端峰. 公钥基础设施(PKI)应用中的信任问题与安全解决方案[J]. 中国安全科学学报,2007,17(10):140-144.

[7] Shi Yanrong, Sun Danning, He Yongqiang, et al. Research and Implementation of Enterprise CA System Based on PKI[C]// International Conference on Management of e-Commerce and e-Government (ICMECG). [s. l.]:[s. n.], 2008.

[8] Wu Jingjing, Jing Jiwu, Lin Jingqiang, et al. A Decentralized Certification Authority Based on Real World Trust Relationships[C]//International Conference on Computer Science and Software Engineering (CSSE). [s. l.]:[s. n.], 2008.

[9] Lioy A, Marian M, Moltchanova N, et al. PKI past, present and future[J]. International Journal of Information Security, 2006,5(1):18-29.

[10] 欧阳宏基,葛 萌,赵 蔷. 基于 JDBC 与设计模式的数据库连接池实现方法[J]. 计算机技术与发展,2011,21(1):84-87.

[11] 孙翠翠,张永胜. 一种改进的基于角色的授权委托模型[J]. 计算机技术与发展,2010,20(11):154-157.

[12] 黄 勤,高东群,刘益良. 工作流系统中基于任务状态的转授权模型[J]. 计算机技术与发展,2011,21(2):34-38.

[13] 中华人民共和国人力资源和社会保障部信息中心. 人力资源和社会保障电子认证体系第 2 部分:电子认证系统技术规范[S]. 2009.

(上接第 238 页)

相应的授权和 WPKI 技术来进一步保证移动电子商务交易过程的安全性。

参考文献:

[1] Tarasewich P. Designing Mobile Commerce Application[J]. Communication of the ACM, 2003,46(12):57-60.

[2] 陈 轶,邓世荣,刘 云. 基于 J2ME 平台的电影票预订系统的设计与实现[J]. 计算机与现代化,2009(7):133-135.

[3] 丁丽梅. 关于移动电子商务安全的研究[J]. 电脑知识与技术,2008(2):966-967.

[4] 代文锋,王玉珍. 我国移动电子商务现状与问题研究[J]. 办公自动化,2008(6):23-24.

[5] 李必云,石俊萍. 基于 WPKI 的移动电子商务研究[J]. 计算机与现代化,2010,175(3):49-51.

[6] 彭 博. 浅谈移动电子商务的信息安全[J]. 农业与技术,2008(6):172-174.

[7] Tang Jian, Terziyan V, Veijalainen J. Distributed PIN Verification Scheme for Improving Security of Mobile Devices[J]. Mobile Networks and Applications, 2003(8):159-175.

[8] 邓 娟,蒋 磊. 3G 网络时代移动电子商务安全浅析[J]. 电脑知识与技术,2009(2):1314-1315.

[9] 吴 章. WAP 协议的安全策略在移动电子商务中的应用[J]. 现代商业,2010(4):189-190.

[10] 范荣真. 基于 WAP2.0 的移动安全支付协议[J]. 技术研究,2010(2):47-48.

[11] 吕福春,陈特放. 基于 WAP 的移动电子商务安全研究[J]. 福建电脑,2008(12):15-16.

[12] 傅杰勇. 我国移动电子商务应用安全问题探析[J]. 中国集团经济,2008(5):65-66.