北京联合大学学术著作出版基金资助

移动商务环境下身份认证机制的研究

Research of Identity Authentication Mechanism in Mobile Commerce

王秦 著

北京交通大学出版社
http://press.bjtu.edu.cn

移动商务环境下身份认证机制的研究

王 秦 著

北京交通大学出版社

·北京·

内 容 简 介

本书分为八章。分别为身份认证机制；移动商务环境下身份认证机制；一次性口令认证机制；椭圆曲线密码体制；基于一次性口令的移动商务身份认证机制的设计；基于一次性口令的移动商务身份认证机制的安全性分析；基于一次性口令的移动商务身份认证机制的仿真；移动商务身份认证评价指标体系的设计。

本书结构合理、内容新颖、理论和实践紧密结合，可作为高等院校信息安全、管理科学与工程等专业本科及研究生教学参考用书，同时也可以作为从事信息安全和计算机仿真的科技工作人员参考用书。

图书在版编目（CIP）数据

移动商务环境下身份认证机制的研究 / 王秦著. —北京：北京交通大学出版社，2012.12

ISBN 978-7-5121-1345-9

Ⅰ.①移… Ⅱ.①王… Ⅲ.①电子商务-身份认证-研究 Ⅳ.①F713.36

中国版本图书馆 CIP 数据核字（2013）第 011561 号

责任编辑：杨 硕 田秀青

出版发行：北京交通大学出版社 电话：010-51686414

北京市海淀区高梁桥斜街 44 号 邮编：100044

印 刷 者：北京鑫海金澳胶印有限公司

经 销：全国新华书店

开 本：140×203 印张：7 字数：175 千字

版 次：2013 年 1 月第 1 版 2013 年 1 月第 1 次印刷

书 号：ISBN 978-7-5121-1345-9/F·1135

印 数：1～700 册 定价：38.00 元

前　言

作为一种移动互联的贸易方式，移动商务将成为全球具有战略意义的贸易手段和信息交换的有效方式。无线通信网络的日益完善、移动设备的普及和广泛应用为移动商务提供了良好的发展机遇，但其面临的安全问题也日渐突出，如通信双方的身份易被假冒，通信内容易被窃听、篡改等。在移动商务的安全机制中，身份认证处于核心地位，在缺乏对身份有效认证的前提下，信息的完整性和保密性没有任何意义可言。因此，移动商务环境下身份认证机制的研究，对移动商务的安全体系，乃至对整个移动商务的推广与发展具有重大意义。

移动商务中常用的身份认证方式是基于用户名/口令的静态口令认证机制，这种认证机制最大的问题是用户名和口令均以明文方式在网络上传输，安全性较低。近年来，随着 PKI 技术的日趋成熟，通过数字证书进行身份认证的应用越来越多。基于数字证书的身份认证机制必须以完整的 CA 体系为基础，但 CA 体系的建设需要投入大量的成本，需要一个合法的、权威的第三方认证机构，同时，移动终端在硬件资源上存在不同程度的限制，这些因素都决定基于数字证书的身份认证机制并不适合于目前国内的移动商务环境。一次性口令认证机制安全性高、实现简单和无须第三方认证，是实现移动商务环境下身份认证机制切实可行的方案。

一次性口令认证机制是一种比较简单的身份认证技术，它可以快速地加载到任何系统之上而无须附加硬件。因为它采用一次一密的方法，可以有效保证用户身份的安全性，同时，它无须第

三方公证、成本低，适合应用于目前尚不成熟的移动商务环境。虽然存在易遭受小数攻击、中间人攻击的安全漏洞，但可以通过椭圆曲线密码体制改进使其安全可靠。结合一次性口令认证机制和椭圆曲线密码体制，设计一套移动商务环境下身份认证机制，旨在可以实现双向身份认证，并能够抵御小数攻击等常见的攻击行为。

目前，移动商务身份环境下认证的研究正处于探索之中。依托国家自然科学基金资助项目“移动商务系统中的身份认证研究”（编号：607730033）、北京联合大学自然科学基金资助项目“基于 OTP 的移动商务身份认证机制的研究”（编号：ZK 201014X）和北京联合大学学术专著出版基金，本书对移动商务环境下身份认证机制进行了一定程度的研究。根据移动商务的环境特点及移动商务环境下身份认证机制的设计需求，设计了基于一次性口令的移动商务身份认证机制，详细阐述注册和登录阶段的流程，通过 BAN 逻辑方法和串空间方法证明机制的安全性，并利用仿真软件 Opnet 对机制进行模拟实现，表明基于一次性口令的移动商务身份认证机制的可行性和高效性。

移动商务环境下身份认证机制的设计本身是一项复杂的工作，需要方方面面的研究和总结。由于本人的知识和研究水平的限制，书中肯定存在纰漏之处，敬请各位老师和专家批评指正，期望在今后的研究中不断完善和改进。

王秦

2012 年 12 月

目　录

第 1 章　身份认证机制 …… 1
1.1　身份认证 …… 1
1.2　身份认证技术 …… 4
1.3　身份认证机制 …… 8
第 2 章　移动商务环境下身份认证机制 …… 16
2.1　移动商务 …… 16
2.2　移动商务的环境特点 …… 25
2.3　移动商务环境下身份认证机制 …… 28
第 3 章　一次性口令认证机制 …… 43
3.1　一次性口令认证机制的实现机理 …… 43
3.2　一次性口令认证机制的分类 …… 50
3.3　一次性口令认证机制的安全性分析 …… 53
3.4　一次性口令认证方案 …… 55
第 4 章　椭圆曲线密码体制 …… 63
4.1　密码体制 …… 63
4.2　椭圆曲线密码体制的基本原理 …… 66
4.3　椭圆曲线密码体制的性能分析 …… 72
第 5 章　基于一次性口令的移动商务身份认证机制的设计 …… 77
5.1　基于一次性口令的移动商务身份认证机制的设计思路 …… 77
5.2　基于一次性口令的移动商务身份认证机制的流程设计 …… 79

第 6 章　基于一次性口令的移动商务身份认证机制的安全性分析 …… 85
6.1　基于一次性口令的移动商务身份认证机制的非形式化分析 …… 85
6.2　基于一次性口令的移动商务身份认证机制的形式化分析 …… 90
第 7 章　基于一次性口令的移动商务身份认证机制的仿真 …… 117
7.1　网络仿真软件 Opnet …… 117
7.2　基于一次性口令的移动商务身份认证机制的仿真建模 …… 137
7.3　基于一次性口令的移动商务身份认证机制的仿真实现 …… 145
7.4　基于一次性口令的移动商务身份认证机制的仿真比较 …… 153
第 8 章　移动商务身份认证评价指标体系的设计 …… 175
8.1　移动商务身份认证评价指标体系 …… 175
8.2　运用模糊综合评价法构建移动商务身份认证评价指标体系 …… 179
附录 A　椭圆曲线生成的代码 …… 193
附录 B　单向散列函数 SHA－1 的代码 …… 198
附录 C　MCIA 机制进程模型的部分代码 …… 204
参考文献 …… 208

第 1 章

身份认证机制

1.1 身份认证

身份认证是最基本的安全服务，其他的安全服务如访问控制、审计都要依赖于它，尤其在开放的网络环境中，必须要对某些需要授权访问的信息进行安全保护，防止非法用户的恶意访问。因此，身份认证对安全的意义重大。

1.1.1 认证

认证（Authentication）是安全业务的基础，它的基本要求为正确性和安全性。认证可以保证信息的真实性和完整性，它是防止主动攻击的重要技术。国际标准 ISO/IEC 9798 - 1 将认证定义为一个实体对另一个实体所称身份的验证。

下面是关于认证的几则定义。

定义 1：认证是对被认证对象的真实性的确认和证明。

定义 2：当被认证的对象是人或机构，被认证的属性是其“身份”，称为“身份”认证。

定义 3：当被认证的对象是一则消息时，认证可以按照被认证的属性分为是否被篡改，称为消息完整性认证；是否被泄露，称为消息机密性认证；是否过时，称为消息新鲜性认证；是否来自正确的信源，称为消息源认证；是否到达目的地，称为消息目

的地认证；是否可读，称为消息可读性认证。

认证通常分为数据源认证（消息认证）和实体认证（身份认证）。消息认证验证信息的完整性，验证数据在传送或存储过程中是否被篡改、重放或延迟等；而身份认证鉴别身份，包括信源、信宿等的认证和识别。

1.1.2 消息认证

消息认证指当接收方收到发送方的报文时，接收方能够验证报文是真实的和未被篡改的。它包含两层含义：一是验证信息的发送者是真正的而不是冒充的，即数据源认证；二是验证信息在传送过程中未被篡改、重放或延迟等。消息认证的检验内容主要包括认证报文的信源和信宿、报文内容是否遭到偶然或有意地篡改、报文的序号是否正确、报文的到达时间是否在指定的期限内。总之，消息认证使接收者能够识别报文的信源、内容的真伪、时间有效性等。这种认证只在相互通信的双方之间进行，而不允许第三者进行认证。

消息认证又称数据完整性校验，检错码和纠错码是检验数据完整性的最简单易行的有效方法。只具有检错功能，但不能确定错误位置，也不能纠正错误，称检错码。具有纠错功能，将无效字码恢复成距它最近的有效字码，但不是 100% 正确，称纠错码。其验证机理如下。

① 密钥生成算法 K，K 是一个生成密钥 k 的随机算法。

② 标签算法 T，由密钥 k 及消息 M 生成标签 $\delta = T_k(M)$。

③ 验证算法 V，由密钥 k、消息 M、标签 δ 验证是否保持数据完整性，输出 1 位 d，$d = V_k(M,\delta)$，要求对于明文空间的所有消息 M 满足：当 $\delta = T_k(M)$ 时，$V_k(M,\delta) = 1$，否则 $V_k(M,\delta) = 0$。

1.1.3 身份认证

身份认证指验证主体的真实身份与其声称的身份是否一致的

过程，其基本思想是通过验证被认证对象的属性，确认被认证对象是否真实有效。身份认证的本质是被认证方有一些信息，除被认证方外，任何第三方不能伪造，被认证方能够使认证方相信他确实拥有那些秘密，则认证他的身份。

通常进行身份认证时，需要主体出示特有的物理特征以证明其身份真实性。身份认证所需的物理特征构成身份认证的物理基础，常用的物理基础包括 3 种。

① 主体所知：主体知道什么，这是基于秘密消息的认证，即认证方根据被认证方提供的信息认证身份，最典型的信息如口令、密码等。

② 主体所有：即令牌认证，认证方根据被认证方提供的某一实物或凭证认证身份，如令牌、证件、证书等。

③ 主体特征：即生物特征认证，认证方根据被认证方的某些特征认证身份，如指纹、虹膜、DNA 等。

与身份认证的物理基础不同，身份认证的数学基础是零知识证明（Zero Knowledge Proof）。零知识证明指使用某种有效的数学方法，使得验证者相信示证者掌握特定的信息，却不泄露任何有用的信息。

零知识证明需要满足以下条件。

① 示证者几乎不可能欺骗验证者，即如果示证者知道证明的知识，他可以使验证者以极大的概率相信他知道证明；如果示证者不知道证明的知识，则他使验证者相信他知道证明的概率几乎为零。

② 验证者无法从示证者得到任何有关证明的知识。

③ 验证者不可能向别人重复证明的过程。

零知识证明通过交互机制实现，验证者 V 向示证者 P 提问，若 P 知道证明则可以正确地回答 V 的提问；若 P 不知道证明，则对提问给出正确回答的概率仅为 1/2。V 以足够多的提问就可以推断 P 是否知道证明，且保证这些提问及相应的回答不会泄漏出 P 所知道的秘密信息。零知识证明比传统的密码技术更安

全并且使用更少的处理资源，但是它需要更复杂的数据交换机制，消耗大量的通信资源。

在整个安全服务中，身份认证主要实现消息的以下性质。

1）完整性

Schneider 定义的完整性为：“对于信息接收者要验证数据在传输过程中没有被修改过，一个入侵者不能用错误的信息去替换合法的信息”。为了检测消息在传输过程中是否被篡改，通常可以采用消息摘要、数字指纹等技术，即在传送的消息中附加信息，接收方对收到的消息进行验证。

2）新鲜性

新鲜性主要用于防止重放攻击，通常可以采用同步机制，如时间戳、同步序列等技术保证消息的新鲜性。

3）不可否认性

不可否认性又称防抵赖性，目的是防止通信的某一方事后抵赖。通常可以采用数字签名、签收机制等技术防止消息双方对消息的发送或接收抵赖。

4）保密性

保密性指为了保证消息在传输过程中不被泄漏，免受其他方窃密。通常可以采取加密技术使消息由明文变成密文。

1.2 身份认证技术

身份认证技术指用户身份的确认技术，可以确认访问者的身份和权限，使访问控制策略可靠执行。目前，身份认证技术主要包括口令认证技术、基于数字证书的身份认证技术、基于物理设备的身份认证技术和基于生物特征的身份认证技术。

1.2.1 口令认证技术

口令认证基于“What you know”的验证手段，是最简单、

最易实现、应用最广泛的认证技术。口令认证技术分为静态口令认证技术和一次性口令（One-Time Password，OTP）认证技术。

静态口令认证技术指用户口令在一定的时间内固定不变、可以重复使用，其认证过程为：登录时，用户输入二元组信息（UserID，UserPW），认证服务器比对接收的信息和存储的信息是否一致，以此判断用户身份的合法性。静态口令认证技术最大的优点是实现简单、易于使用，但其存在诸多安全问题。

① 静态口令认证技术是一种单因子的认证技术，安全性仅依赖于口令，口令一旦泄露，安全性随即丧失。

② 静态口令是固定不变的，难以抵御重放攻击。

③ 静态口令通常比较简单，难以抵御口令猜测攻击。

④ 口令在传输过程中易被截获，难以抵御窃听攻击。

⑤ 通常用户口令以文件形式存储在认证服务器，攻击者可以利用系统漏洞获取口令文件。即使口令经过加密后存放在口令文件中，如果口令文件被窃取，可以进行离线字典攻击。

⑥ 静态口令认证技术是单向认证机制，即服务器对登录用户的身份认证，而用户无法认证服务器，因此，攻击者可能伪装成认证服务器欺骗用户。

OTP 认证技术建立在密码学基础之上，通过在认证过程中加入不确定因子，使用户每次进行身份认证的认证口令都不相同，而且每个认证口令只使用一次。OTP 认证技术的一次一密的认证方法可以有效保证用户身份的安全性。

与静态口令认证技术相比，OTP 认证技术的主要特点包括以下方面。.

① 动态性：一次性口令可以随设定的时间或事件等变量自动变化，无须人工干预。

② 一次性：口令一次有效，使过的口令不能重复使用，即使口令被窃听，也不会造成很大的危险，因此，其具备良好的抗窃听性。

③ 随机性：一次性口令随机生成、无规律，增加了破解的难度。

④ 多重安全性：与静态口令的单一认证方式不同，OTP 认证技术将一次性口令与用户名、静态口令等多重因素结合实现认证。

1.2.2 基于数字证书的身份认证技术

随着 PKI 技术的日趋成熟，通过数字证书进行身份认证的应用越来越多。基于数字证书的身份认证技术可以对传输的信息进行数字签名，保障信息的机密性和完整性、交易实体身份的真实性及签名信息的不可否认性。

数字证书（Digital Certificate）是标志用户身份的一系列特征数据，一般包括证书版本、序列号、用户公开密钥、证书所用的数字签名算法说明等。数字证书由权威公正的第三方机构即 CA 中心签发。基于数字证书的身份认证技术的认证过程为：CA 中心为某一用户 A 颁发证书，并用自己的私钥对证书签名，另一用户 B 想验证 A 的身份时，利用 CA 中心的公钥验证 A 的数字证书的完整性，从而判断 A 是否是合法用户。

基于数字证书的身份认证技术具备较高的安全性，但其存在一些问题，如成本较高；用户私有密钥保存的安全问题；用户用于取出私钥的通行字的质量问题；证书废止与证书废止列表（Certificate Revocation List，CRL）刷新的时间差问题。最重要的是目前国内还没有一家法律上承认的权威第三方 CA 中心，这是 PKI/WPKI 认证技术在国内应用发展的主要瓶颈。

1.2.3 基于硬件设备的身份认证技术

基于硬件设备的身份认证技术指用户通过随身携带身份认证令牌进行身份认证的技术，通常需要与其他身份认证技术一起使用。例如，银行的 ATM 卡必须要有口令即用户的 PIN（Personal

Identification Number）码，才能从 ATM 机上提取现款。目前应用最广泛的身份认证令牌设备是智能卡。智能卡内部包含 CPU 和存储器，能够进行特定运算并且存储数据。

基于硬件设备的身份认证技术的主要优点是能够存储足够大的信息，而且不容易被复制。与基于口令的认证技术相比，它能够提供更高的安全性，一旦身份认证令牌遗失或被盗，攻击者不知道 PIN 码也无法使用令牌。但这种身份认证技术需要硬件设备，因此成本较高，同时，其无法抵御口令猜测攻击。

1.2.4　基于生物特征的身份认证技术

基于生物特征的身份认证技术指提取具有唯一性的生理特性或行为方式作为认证依据，其认证过程分为四个步骤，即生物特征提取、特征模板生成、特征测量与比较、特征匹配。

与其他身份认证技术相比，基于生物特征的身份认证技术的特点为以下方面。

① 随身性：生物特征是人体固有的特征，与人体唯一绑定，具有随身性。

② 安全性：人体特征本身就是个人身份的最好证明，能够满足更高的安全需求。

③ 唯一性：个体拥有的生物特征各不相同。

④ 稳定性：生物特征如指纹、虹膜等不会随时间等条件的变化而变化。

⑤ 方便性：基于生物特征的身份认证技术无须记忆密码或使用特殊工具（如钥匙），不会遗失。

从理论上说，生物特征几乎无法被冒用或造假，因此，与其他身份认证技术相比，基于生物特征的身份认证技术的安全性和可靠性是最高的。但这种身份认证技术目前还不够成熟，同时，其存在识别设备成本高、稳定性差等问题，不适合移动商务环境下身份认证。

从上述身份认证技术的特点可以看出，OTP 认证技术实现简单、成本低、无须第三方认证，同时一次一密保证了较高的安全性，比较适合移动商务环境下身份认证。

1.3 身份认证机制

身份认证是验证主体的真实身份与声称的身份是否一致的过程，这一过程通过特定的机制和算法实现。身份认证的功能通过身份认证机制实现。

1.3.1 认证机制

认证机制（Authentication Mechanism）指在各认证主体之间如何分发机密信息，以及如何利用机密信息对主体身份进行认证的机制。认证机制建立在密码学基础上，其目标在于证明其声称的某种属性。

Paul C. 将认证机制的目标归纳如下。

① G1：远端处于工作状态（Far-end Operative）

$$A \mid \equiv B \text{ say } Y$$

② G2：目标实体验证（Targeted）

$$A \mid \equiv B \text{ say}(Y, R(G(RA), Y)$$

③ G3：安全密钥建立（Secure Key Establishment）

$$A \mid \equiv A \overset{K_-}{\longleftrightarrow} B$$

④ G4：密钥确认（Key Confirmation）

$$A \mid \equiv A \overset{K_+}{\longleftrightarrow} B$$

⑤ G5：密钥新鲜性（Key Freshness）

$$A \mid \equiv \#(K)$$

⑥ G6：对共享密钥的相互信任（Mutual Belief in Shared Secret）

$$A \mid \equiv (B \mid \equiv A) \xleftrightarrow{K_{-}} B$$

1. 认证机制的分类

认证机制可以按照如下方式进行分类。

1）基于实体间的关系

根据参与认证实体间的关系，认证机制可以分成单向认证和双向认证。在单向认证机制中，一方必须向另一方提供用于验证的信息，证明方只能无条件地信任验证方。在双向认证机制中，参与认证的各方处于平等的地位，各方为了取得对方的信任必须提供自己的身份证明信息。

2）基于认证信息的性质

根据认证信息的性质，认证机制可以分为秘密知识证明、物理介质证明和实体特征证明。秘密知识证明主要通过通信双方共同掌握的秘密信息来进行身份验证，包括口令、个人识别码、密钥等。在物理介质证明中，证明方提供拥有的物理介质进行身份验证，主要包括令牌卡、信用卡、密钥卡等。实体特征证明包括两个方面，首先是实体的物理特征，例如，计算机等通信设备的机器识别码、网卡 MAC 地址、硬盘序列号等，还有个人的生物特征，包括手形、指纹、虹膜、视网膜、声音等。

3）基于认证对象的分类

根据认证对象的分类，认证机制可以分为身份认证和信息认证。身份认证主要鉴别实体的真实身份；信息认证用于消息传递过程中的完整性、新鲜性和不可抵赖性的认证。

4）基于通信双方的信任关系

根据通信双方的信任关系，认证机制可以分为有仲裁认证和无仲裁认证。在无仲裁认证机制中，通信双方是互相信任的，他们共同抵御敌方的攻击；在有仲裁认证机制中，通信双方是互不信任的，在通信过程中任何一方都有可能作弊，一旦出现纠纷，需要可信的第三方进行仲裁。此通信系统共有四方参与，即发方、收方、敌方和仲裁方。

2. 评价认证机制的标准

评价某一认证机制，可以遵循以下几个标准。

1）可行性

从用户的观点看，认证机制应提高用户访问应用的效率，减少多余的交互认证过程，提供一次性认证。所有用户可访问的资源应提供友好的界面。

2）认证强度

认证强度取决于采用加密算法的复杂度及密钥的长度。算法越复杂、密钥越长，机制的认证强度越高，机制的安全性越好，但同时要考虑加密时间、用户所能忍受的时间限度。

3）认证粒度

身份认证只决定是否允许用户进入服务应用。认证后如何控制用户访问的内容，以及控制的粒度也是认证机制的重要标志。

4）认证数据正确

消息的接收者能够验证消息的合法性、真实性和完整性，而消息的发送者对所发的消息不可抵赖。除合法的消息发送者外，任何其他人不能伪造合法消息。

1.3.2 身份认证机制

身份认证通过特定的机制和算法实现。身份认证机制指认证双方约定采用一定的身份认证技术进行身份认证的机制，它定义了参与认证的通信方在身份认证过程中需要交换的消息的格式、消息发生的次序及消息的语义。

身份认证机制可以根据不同的划分标准进行分类。根据机制涉及的主体数目划分为两方身份认证机制（认证双方）和三方身份认证机制（认证双方和认证服务器）；根据认证的方式划分为单向身份认证机制和双向身份认证机制；根据认证的目的划分为只完成主体认证功能的身份认证机制、完成主体认证和密钥分配双重功能的身份认证机制；根据使用的密码技术划分为基于对