

云计算环境下基于二维码的移动终端身份认证方案

马立林

(九江学院 信息技术中心, 江西 九江 332005)

摘 要: 提出一种云计算环境下的移动终端身份认证方案, 用于解决传统身份认证技术中存在的不足. 该方案以二维码为信息传输载体, 结合动态加密密钥、对称加密算法和不可逆函数, 实现了移动终端的动态认证. 通过安全性分析可知, 该方案结构简单, 不需要借助第三方设备, 具有较高的安全性和适应性.

关键词: 云计算; 二维码; 移动终端; 身份认证; 动态密钥; MAC; IMSI

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2016)01-0140-04

An Identity Authentication Scheme of Mobile Terminal Based on Two-Dimension Code in Cloud Computing Environment

MA Li-lin

(Information Technology Center, Jiujiang University, Jiujiang 332005, China)

Abstract: With the rise of cloud computing and the wide use of mobile platforms, this paper presents a mobile terminal authentication scheme in cloud computing environment, which is used to solve the problems of security in the traditional identity authentication technology. The programme with two-dimension code for information transmission carrier, combined with dynamic encryption keys, symmetric encryption algorithm and an inverse function. It realized the dynamic authentication of mobile terminal finally. According to the security analysis, the scheme with higher security and flexibility provides a simple structure and does not depend on third-party devices.

Key words: cloud computing; two-dimension code; mobile terminal; identity authentication; dynamic key; MAC; IMSI

1 引言

随着移动终端技术和移动互联网技术的快速发展, 移动平台对信息处理的能力得到了显著提高. 如今, 广泛使用的智能手机、平板电脑等各移动平台已渗透到日常生活和工作中, 特别是在新兴的物联网和云计算方面具有广阔的应用前景^[1].

云计算是一种基于互联网, 融合多种计算技术, 按需订阅服务和付费的创新模式. 传统信息化应用环境中的安全问题^[2], 比如撞库、暴力破解、账号被盗、重放攻击等依然存在. 针对这些安全问题, 传统的认证方式有 PKI 技术、动态口令技术、一次性密码卡技术等. 如文献^[3]使用 USBKEY 身份认证,

文献^[4]使用基于挑战响应机制的动态口令技术, 文献^[5]使用动态口令产生分离的动态口令技术等. 但目前一些云计算平台依然采用静态口令技术, 其登录信息容易被非法截取. 移动平台在带给大家丰富多彩的应用和方便快捷的生活的同时, 其安全问题依然不容乐观. 目前静态口令认证仍然是移动应用普遍采用的方式, 其存在不易控制安全性, 容易被盗取、撞库、猜测和穷举攻击, 已成为制约信息化发展的一个主要瓶颈. 然而在云计算环境下, 用户登录时的身份认证是进入移动平台的入口, 起着至关重要的作用. 因此有必要设计适用于移动平台且安全方便的身份认证方案^[1].

2 二维码技术

2.1 二维码概述

二维码即二维条形码,是指用某种特定的几何图形,按一定规律在二维平面分布的黑白相间的图形上记录信息^[6].借助于“0”、“1”比特流的概念对所表示的信息进行编码,不同的图像、文字和数值对应于不同的用二进制位所表示的几何图形,是一种全新的信息存储、传递和识别技术.能够用来表示多种类型信息,比如:不同国家的语言文字、数值信息、图像信息等,其具有高容量、高密度、纠错能力强、快速定位与自动编解码等特点^[7].

QR 码是二维码中的一种编码技术,是一种矩阵式二维码符号^[8],具有以下特点.(1)存储容量大是一维码容量的数十倍.能够储存近 2 000 个汉字,或者大约 7 100 个数字,或者 4 200 个英文字母.(2)编码范围广:既可以表示图文信息,又可以表示声像信息.鉴于 QR 码的特点,本文选用 QR 码作为信息载体用来存储更多具有用户本身特征的信息,增强身份认证功能,提高移动终端上使用云计算系统的安全性.

2.2 二维码的编码及译码流程

本文采用 QR 编码技术做为二维码的处理技术,主要包含编码和译码过程,如图 1、图 2 所示.同时考虑到二维码所含信息的安全性,避免被任一二维码工具解码,利用对称加密算法和动态密钥对生成二维码的信息进行加密处理,只有特定的解码程序才能正确读取二维码的信息.

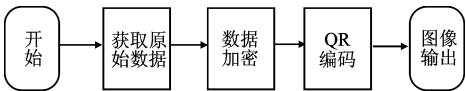


图 1 二维码编码流程图

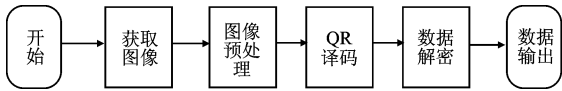


图 2 二维码译码流程图

3 基于动态密钥和二维码的认证方案

本方案以移动终端具有唯一性的 Media Access Control (MAC) 地址, International Mobile Subscriber Identification Number (IMSI) 和服务端的 MAC 地址作为身份认证的主要认证因素,在利用 Network Time Protocol (NTP) 技术实现移动终端

与服务端时间同步的前提下,针对 IMSI、系统时间和用户访问次数,运用不可逆的单向散列函数、分组转制、异或、取位等操作,产生用于对称加密的动态密钥,并通过现在广泛使用的二维码和对称加密算法两次加密需要认证的信息,最终在服务端、移动终端分别实现了对对方的认证.

3.1 用户注册过程描述

用户若想使用公有云提供的服务,需首先向云平台进行注册,比如百度云、腾讯云和阿里云.为了保证注册的安全性,从源头加强安全性控制,以及为后面的身份认证提供基础支持,提出了一种新的注册方法,注册申请过程如图 3 所示.

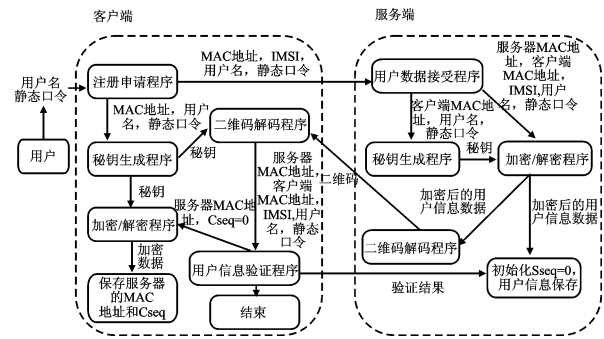


图 3 注册申请流程图

具体步骤如下所示.

(1)先登录公有云网站或通过扫描二维码下载移动客户端.

(2)用户通过输入设备输入用户名 (UserName) 和静态口令 (PassWord).

(3)移动终端利用不可逆算法分别对移动终端 MAC 地址 (str_MacAddr)、UserName 和 PassWord 产生三个固定位长的摘要,然后进行分组转制,异或和取位等运算产生用于对称加密的动态密钥 c_save_Key.

$$c_save_Key = f_{key}(str_MacAddr, UserName, PassWord) \quad (1)$$

(4)注册申请程序使用双方共享的对称密钥,运用对称加密算法对读取的移动终端 MAC 地址、IMSI (str_ImsiNum), 和输入的 UserName 和 PassWord 实施加密,产生加密信息 (rs_Encrypt_Info), 并发送给服务端.

$$rs_Encrypt_Info = f_{aes}(str_MacAddr, str_ImsiNum, UserName, PassWord) \quad (2)$$

(5)服务端使用双方共享的对称密钥解密移动终端发送过来的信息,同时采用与移动终端相同的不可逆算法分别对 str_MacAddr、UserName 和

PassWord 产生三个固定位长的摘要, 然后进行分组转制、异或和取位运算产生用于对称加密的动态密钥 s_save_Key , 与步骤(3)相同。

(6) 服务端初始化服务端用户访问次数 $Sseq=0$, 并采用步骤(5)所产生的动态密钥, 通过对称加密算法加密移动终端 MAC 地址, IMSI, UserName, PassWord, 服务端 MAC 地址和 $Sseq$, 同时调用数据库程序保存加密后的移动终端 MAC 地址, IMSI, UserName, PassWord 和 $Sseq$ 。

(7) 服务端调用二维码生成程序对步骤(6)加密后的信息, 生成一个二维码发送到移动终端, 并在发送完毕后删除二维码。

(8) 移动终端接收服务端发送的二维码, 调用二维码解码程序对二维码进行解码。

(9) 移动终端采用步骤(3)所产生的动态密钥, 通过对称加密算法对解码出的二维码信息进行解密, 并把解密出来的信息与移动终端的 MAC 地址, IMSI, UserName, PassWord 进行比较. 如果一致就表示注册成功, 否则, 提示注册失败。

(10) 如果步骤(9)中的反馈注册成功, 移动终端初始化客户端用户访问次数 $Cseq=0$, 并采用步骤(3)所产生的动态密钥, 通过对称加密算法加密服务端 MAC 地址和 $Cseq$, 且保存在客户端, 同时删除服务端发送过来的二维码。

3.2 身份认证过程

身份认证是一个系统的安全基础, 已受到大量研究者的关注, 产生了大量的研究成果. 然而, 经研究发现, 大部分文献中的身份认证过程采用单向认证, 即服务端的认证, 很少考虑客户端的认证, 比如文献[9]等. 虽然服务端的认证能够对来自客户端的用户进行身份识别, 拒绝非法身份的访问, 但如今的用户越来越容易受到服务端的欺骗攻击, 比如钓鱼网站, 通过模仿真实网站盗取用户的用户名、密码、银行卡号和身份证号等. 怎样防止欺骗攻击越来越受到关注和重视, 加强客户端的认证已成为一种有效手段. 针对以上问题, 在基于服务端认证的基础上, 提出了一种新的认证方法, 加强了客户端的认证, 整个身份认证过程如图 4 所示。

3.2.1 服务端认证

(1) 在移动终端的客户端程序登录界面上通过输入设备输入 UserName 和 PassWord, 利用对称算法和双方共享的对称密钥加密 $str_MacAddr$ 、UserName 和 PassWord, 并通过登录程序将加密信息发送到服务端的登录验证程序。

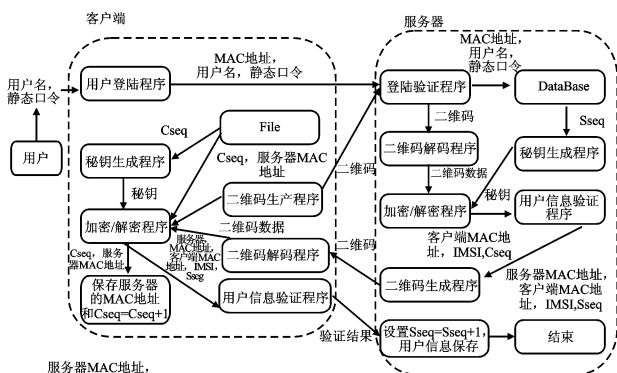


图 4 移动终端、服务端认证流程图

(2) 服务端验证程序对移动终端发送过来的加密信息进行解密, 同时利用不可逆算法分别对解密出来的 $str_MacAddr$ 、UserName 和 PassWord 产生三个固定位长的摘要, 然后进行分组转制、异或和取位运算产生动态密钥 s_save_Ke 。

$$s_save_Key = f_{key}(UserName, PassWord) \quad (3)$$

(3) 以用户名为检索条件, 在数据库中检索出用户密码, 并以(2)产生的动态密钥 s_save_Key 为解密密钥对用户密码解密, 比较密码是否一致, 并给移动终端发送验证结果信息。

(4) 如果(3)验证通过, 移动终端利用不可逆算法分别对 $str_MacAddr$ 、UserName 和 PassWord 产生固定位长的摘要, 然后进行分组转制、异或和取位运算产生动态密钥 c_save_Key , 否则, 提示认证失败。

(5) 利用(4)产生的动态密钥 c_save_Key 解密移动终端保存的加密文件, 读取 $Cseq$ 。

(6) 移动终端利用不可逆算法分别对移动终端 IMSI、用户访问次数 $Cseq$ 和系统时间进行单向散列计算, 产生三个固定位长的十六进制摘要, 然后进行分组转制、异或和取位运算产生动态密钥 $c_er_code_Key$ 。

$$c_er_code_Key = f_{er_key}(str_ImsiNum, systime, Cseq) \quad (4)$$

(7) 移动终端采用(6)产生的动态密钥 $c_er_code_Key$, 通过对称加密算法对 $Cseq$ 、客户端 MAC 地址和 IMSI 加密, 并调用二维码生成程序产生二维码, 发送到服务端。

(8) 服务端接收二维码、解码, 并对解码出的信息进行解密, 与服务端存储的客户端 MAC 地址, IMSI, $Sseq$ 比较. 如果一致, 则通过服务端验证, 否则, 拒绝。

3.2.2 移动终端认证

(1)在通过服务端验证后,服务端利用不可逆算法分别对移动终端 IMSI、用户访问次数 Sseq 和系统时间进行单向散列计算,产生三个固定位长的十六进制摘要,然后进行分组转制,异或和取位运算产生动态密钥 s_er_code_Key.

$$\begin{aligned} & s_er_code_Key = \\ & f_{er_key}(str_ImsiNum, systime, Sseq) \end{aligned} \quad (5)$$

(2)服务端采用(1)产生的动态密钥 s_er_code_Key,通过对称加密算法加密服务端的 MAC 地址,移动终端的 MAC 地址,IMSI,Sseq,用户名和静态口令,并调用二维码生成程序生成二维码,发送到移动终端.

(3)移动终端接收服务端发送过来的二维码、解码,并对解码的信息进行解密,与移动终端存储的服务端 MAC 地址、Cseq,本地读取的移动终端 MAC 地址、IMSI,以及输入的用户名和静态口令比较,如果一致,则通过移动终端认证,否则,拒绝.

(4)如果(3)认证通过,分别在移动终端修改 Cseq 的值, $Cseq = Cseq + 1$,服务端修改 Sseq 的值, $Sseq = Sseq + 1$,并加密保存及删除二维码,否则,提示认证失败及删除二维码.

4 安全性分析

本方案具有较高的安全性,具体分析如下.

(1)移动终端 MAC 地址、用户名和密码等信息采用 128 位长的共享密钥,通过对称加密算法加密传输,提高了数据传输的安全性.

(2)移动终端和服务端的数据保存采用由用户名和密码,经不可逆算法、分组转制、异或、取位运算产生的动态密钥加密,每个用户具有不同的密钥,确保了保存数据的安全性.

(3)通过二维码传输的信息采用由移动终端 IMSI,系统时间,用户访问次数,经不可逆算法、分组转制、异或、取位运算产生的动态密钥加密.同一用户每次传输所采用的加密密钥不一致,每个用户所采用的密钥也不一致,即使二维码被截获,也无法获取二维码隐藏的信息,从而保证了二维码信息的安全性.

(4)用于加密二维码信息的动态密钥具有复杂性和动态性,并在云服务端和移动终端同时产生,以避免在网络传播过程中被窃取.

(5)在实现服务端对移动终端认证的基础上,在移动终端上增加了对服务端的认证,避免了传统认

证方案中对服务端认证的缺失,在安全性上得到了进一步的提高.

(6)抵御中间人攻击:在服务端以二维码为信息载体与移动终端通信时,若二维码被攻击者截获并冒充合法用户与服务端通信,由于攻击者无法获得移动终端的 MAC 地址、IMSI,而程序自动读取移动终端的 MAC 地址、IMSI,并与二维码隐藏的 MAC 地址、IMSI 进行比较,因此能够有效防御中间人冒充合法用户进行攻击.

(7)抵御重放攻击:服务在每次启动时都重新产生新的加密密钥和生成新的二维码信息,并且在每次认证通过后,都会把本地的二维码删除.这样,若想获得用于攻击的有用信息将变得很难,即便能够获取相关信息,也会因为只使用一次而变得不可以重用.

(8)抵御小数攻击:利用 SHA1 产生基于多因子的加密密钥,具有不可逆性、不重复性和一次性,能够有效抵御传统方案中存在的小数攻击.

5 结束语

本文提出了一种云计算环境下的移动终端身份认证方案,该方案融合了动态密钥、对称加密和二维码等技术.所有传输信息都经过加密处理,且加密密钥是采用具有移动终端具有唯一性的 MAC 地址、IMSI,以及系统时间和用户访问次数等动态信息、通过不可逆算法、分组转制、异或和取位等运算产生,保证了加密密钥的唯一性和动态性,能够抵御重放攻击、小数攻击和撞库等安全威胁.同时在实现传统服务端认证的基础上,实现了移动终端的认证,能够抵御中间人攻击,具有较高的安全性.

参考文献:

- [1] 胡卫,张焕国,魏国珩,等.面向移动平台的新型身份认证方案设计[J]. 计算机科学,2014,41(4): 99-102.
- [2] 徐祺.基于数字证书的云计算安全认证平台的研究[J]. 计算机安全,2013,13(7):67-70.
- [3] 王帅,常朝稳,魏彦芬.基于云计算的 USBKey 身份认证方案[J]. 计算机应用研究,2014,31(7):2130-2134.
- [4] 刘昌明,马艳,宗文富.基于挑战_响应机制的动态口令系统的设计[J]. 计算机与数字工程,2012,40(12): 112-115.
- [5] 王伟珣.基于手机及挑战响应机制的动态口令系统研发[D]. 上海:上海交通大学,2013.

(下转第 148 页)

过基于 GMM-UBM 说话人识别系统进行说话人识别. 实验结果表明,混合参数在不增加复杂度的同时能够得到更高的识别率,鲁棒性更好. 本文选择的高斯混合模型为 16 阶,但如果能自适应选择混合阶数,进一步提高系统的识别率,将是下一阶段研究的重点.

参考文献:

[1] 赵力. 语音信号处理[M]. 北京:机械工业出版社,2012

[2] 柯晶晶,周萍,景新幸,等. 差分 and 加权 Mel 倒谱混合参数应用于说话人识别[J]. 微电子学与计算机,2014,31(9):89-91

[3] Radhak R Ishnan R, Divakaran A. Systematic acquisition of audio classes for elevator surveillance [C] // SPIE Image and Video Communications and Processing. San Jose CA: SPIE, 2005:64 -71.

[4] 吴迪,曹洁,王进花. 基于自适应高斯混合模型与静动态听觉特征融合的说话人识别[J]. 光学精密工程, 2013,21(06):1598-1604.

[5] 王伟,邓辉文. 基于 MFCC 参数和 VQ 的说话人识别系统[J]. 仪器仪表学报,2006,27(6):2253-2155.

[6] Zhou Ping, Li Xiaopan, Li Jie, et al. Speech emotion recognition based on mixed MFCC[C]// International Conference on Applied Mechanics and Mechanical Engineering. [s. l.]:IEEE, 2012:1252-1258.

[7] Teager H, Teager S. Evidence for nonlinear sound production mechanisms in the vocal tract[M] // Speech Production & Speech Modeling. [S. l.]: Springer, 1990:241-261.

作者简介:

王茂蓉 女,(1990-),硕士研究生. 研究方向为语音识别与反蓄意模仿. E-mail:13737726138@163. com.

周 萍 女,(1961-),硕士,教授. 研究方向为语音识别与智能控制研究.

景新幸 男,(1960-),硕士,教授. 研究方向为语音识别及其混合集成电路设计等研究.

(上接第 143 页)

[6] 林玮,王晓峰. 基于非齐次线性方程组的一次性口令认证协议[J]. 计算机工程,2010,36(13):154-158.

[7] 桂振文,王涌天,刘越,等. 二维码在移动增强现实中的应用研究[J]. 计算机辅助设计与图形学学报,2014,26(1):34-39.

[8] 国家质量技术监督局. GB/T 18284-2000-快速响应矩阵码[S]. 北京:中国标准出版社,2001.

[9] 薛凯,李海霞,杨树国. 一种针对云计算登陆问题的认证技术[J]. 科学技术与工程,2011,11(6):1375-1377.

作者简介:

马立林 男,(1977-),硕士,高级工程师. 研究方向为云计算、信息安全. E-mail:malilin@126. com.