# 二维 QR 码在电子商务中应用的安全性研究

张 丰,施 勇,薛 质
(上海交通大学 电子信息与电气工程学院 上海市信息安全综合管理技术研究重点实验室,
上海 200240)

**摘 要**:近年来,二维 QR 码在电子商务中的应用越来越广泛,但是随之也出现了许多关于二维码的安全问题。因此,主要采用文献调研以及实验实践的方法,研究了二维 QR 码在电子商务中的应用以及安全性问题。对二维 QR 码的构成、来源、特点进行了概述,对二维 QR 码在当今电子商务中各个方面的应用,如安全登录、扫描购物、电子凭证、二维码支付等,进行了介绍,并对二维 QR 码在电子商务应用中的安全性问题,如物理攻击、隐私泄露、扫描攻击等,进行了总结。从信息安全具体的安全属性出发,总结和提出了对二维码内容进行加密、对发布者发布的二维码提供身份认证机制这两大改进方向。

**关键词**:二维 QR 码;电子商务;安全性研究
**中图分类号**:TP393 **文献标识码**:A **文章编号**:1673-629X(2017)03-0131-05
doi:10.3969/j.issn.1673-629X.2017.03.027

# Research on Security of Application of 2-Dimentional QR Code in Electronic Commerce

ZHANG Feng, SHI Yong, XUE Zhi
(Key Laboratory of Integrated Administration Technologies for Information Security of Shanghai,
School of Electronic Information and Electrical Engineering of Shanghai Jiaotong University,
Shanghai 200240, China)

**Abstract**: In recent years, the application of 2-Dimentional (2D) QR code has more and more extensive in E-commerce, accompanying with many security issues. Hence, the application and security issue of QR code in the E-commerce are studied by means of document research and experiment. The formation, origin and features of 2D QR code are summed up, diverse applications of QR code in current E-commerce including secure login, scanning shopping, electronic certificate, 2-Dimensional code payment are introduced, and the emerging security issues such as physical attacks, privacy divulging, scanning attacks and so on summarized. Finally, by referring the attributions of information security, two improving ways of encryption of 2D code contents and offering authentication of the issued specific 2D code are summed up.

**Key words**: 2-Dimentional QR code; E-commerce; security study

## 0 引 言

电子商务经过 10 多年的发展,如今已成为人们生活中必不可少的一部分。它创造了大量的就业岗位,推动了经济发展,更孕育出了像阿里巴巴、支付宝这样的互联网巨头。电子商务在 PC 互联网上已相当成熟,各大公司纷纷把新的战略要点聚集在移动互联网上。

而近年来,带摄像头的触屏智能手机的普及,带动了许多新的技术应用,如手机购物、手机支付、打车软件、二维码支付等等。二维码得益于智能手机的发展,在电子商务的各领域得到了应用,像在日本和韩国,近 8 成手机用户通过手机“扫描上网”和购买电子票据。在中国,像二维防伪码,演唱会二维电子票,地铁站通道的二维码购物墙,手机支付宝的扫一扫转账,付款码,报纸杂志上的广告二维码,等等[1-3],随处可以找到。在中国广泛使用的二维码基本上是日本 Denso-

**收稿日期**:2015-12-08 **修回日期**:2016-04-13 **网络出版时间**:2017-02-17
**基金项目**:国家自然科学基金资助项目(61332010)
**作者简介**:张 丰(1990-),男,硕士,研究方向为电子商务信息安全;薛 质,教授,研究方向为信息安全。

Wave 公司发明的 QR(Quick Response)码,正如其名,相比于其他二维码有快速识别,360°拍摄读取无限制,高密度,大容量,抗污损能力强等优点。

在二维码给人们带来便利、新颖的好处时,许多问题也伴随而来。如火车票最开始应用二维码时的泄露信息问题,有报道的手机扫一扫二维码,手机话费被扣光问题,支付宝账号被盗问题,等等。由此,研究二维码的安全性就有了非常重大的意义。

## 1 二维 QR 码简介

二维码是按一定规律在平面上(二维方向)分布黑白像素的特定图形。相对于一维条形码只能在一个方向分布信息,二维码具有密度大,能承载大量信息的优点。常见的二维码有行排列式二维码 CODE49、PDF417,矩阵式二维码 Data Matrix、QR Code 等。矩阵式二维码在矩阵元素位置上,出现黑色(也支持其他颜色)方点表示二进制“1”,不出现点表示二进制“0”,点的排列组合确定了矩阵式二维码所代表的意义。

QR 码于 1994 年由日本 Denso-Wave 公司发明,QR 码的标准 JIS X 0510 在 1999 年发布,而其对应的国际标准是 ISO/IEC18004。QR 码是属于开放式的标准,其规格公开,而由 Denso Wave 公司持有的专利权益,并不会被执行,所以世界各国纷纷采用了 QR 码技术。国内在原标准基础上进行适当修改,于 2000 年发布了相对应的国家标准 GB/T18284。

图 1 是版本等级 2 的 QR 图,它是 25 * 25 规格的。QR 码提供了 40 个版本,最小的版本是 21 * 21 模块的,最大的版本则是 177 * 177。

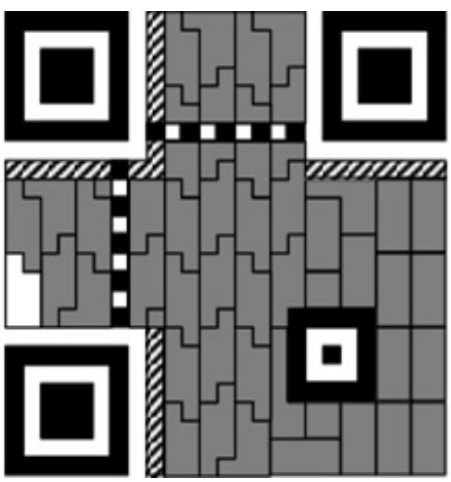

图 1 QR 码版本二

图中的左上角、左下角和右上角的 3 个“回”字结构是 QR 码的位置探测图形,用于快速识别图形方向,它可以使拍摄时不受角度限制;而右下角的 1 个“回”字结构是校正图形,用于确定和校正符号中模块的坐标;另外,QR 码可以根据实际需要,灵活选择纠错等级。QR 码按纠错等级分为 4 等,分别有 7%,15%,25% 的码字被纠正。其他更多信息请参见文献[4],它是国内的 QR 码标准。

## 2 QR 码在电子商务中的应用

QR 码主要和手机一起使用,根据其具体使用方式的差别,将其分为主读类应用和被读类应用。被读类应用主要将手机作为接收和存储 QR 码的地方,需要由其他设备来识别读取二维码信息,读取信息之后的业务也不在手机上执行。典型的应用如电子优惠券、电子会员卡等。主读类应用是手机安装有二维码识读软件,并用手机摄像头识读二维码,在手机本地解析或者通过网络与相应系统数据库进行交互处理,然后再执行具体的业务。下面将介绍 QR 码在电子商务中的几大类典型应用。

### 2.1 安全登录

长久以来,在登陆网站的方式是登录名和密码。但是,当想在公共场所(比如网吧)登录淘宝网时,会有很多安全险患。然而现在很多购物网站(像淘宝网)提供了 QR 码登录方式,具体流程如图 2 所示。

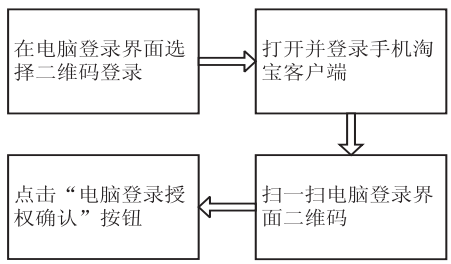


图 2 QR 码安全登录流程

根据流程图可知,在电脑上登录淘宝网的过程中,并没有在电脑上输入任何信息,登录信息是通过手机网络(不要走 Wifi 网络,走 3G 网络更安全)进行的,相对来说比较安全。其具体的实现原理是,网站上的二维码内容有一个独特的标识序列,用户用登录的手机扫描后,会将这个唯一的标识序列发送到网站的服务器。服务器接到消息后,确认登录的手机客户端的身份,然后将登录的网站展现给用户[5]。

### 2.2 商品防伪溯源

以往,若要辨别一个商品的真伪需要记下商品的防伪码,然后到商品对应官网或国家食品(产品)安全追溯平台进行查询[6],有时并不方便。现在淘宝手机客户端已经支持“中国药品电子监管码”的查询,经扫描条码后,可以查到药品自被生产出来后的流转信息。手机软件应用市场的“我查查”软件也提供类似的防伪溯源功能,此外,它还提供比价功能,展示该产品在附近商场超市的不同价格。而类似 QR 码能够承载更多的信息,以后会支持更多商品的防伪溯源查询。

### 2.3　电子凭证

现代生活中,人们离不开各种卡券,然而卡券多了以后,携带不便,易于丢失,而且卡券本身也有成本,补办麻烦。而二维 QR 码电子卡券就解决了很多问题,它携带方便,几乎无成本,像绑定支付宝的世纪联华电子卡,银泰电子卡,即使丢失手机,也不会丢失卡。这样的例子有电子会员卡、电子提货券、电子优惠券、电影票电子券等。现在支付宝手机钱包的“服务号”栏目就提供了很多实体商店的公众号,也绑定了用户的电子卡券,这将线上营销和线下使用相结合,具有很强的发展趋势。

### 2.4　二维码“扫描购物”

在各家互联网公司争夺移动互联网入口的战争中,二维码是极为重要的一个战场。淘宝网制订了“码上淘”战略,在其网址 www. ma. taobao. com 上,淘宝卖家可以根据需要生成多种 QR 商品码、媒体码、服务码、店铺码等。腾讯公司的微信也推出了微信二维码。在很多报纸杂志,商品包装上可以看到很多二维码广告,还有地铁通道的二维码购物墙等等。究其本质来说,这些二维码信息提供的只是一个网址,但是网址手动输入易输错并且耗时,而手机“扫一扫”却极为方便,这使得扫描购物极为流行。

### 2.5　二维码支付

根据支付宝的解释,二维码支付是商家将账号商品价格等一系列信息汇编成一个二维码,用户通过移动手机终端扫拍二维码便可实现支付结算的体系。2014 年 3 月 13 日,央行下达《中国人民银行支付结算司关于暂停支付宝公司线下条码(二维码)支付等业务意见的函》,叫停了二维码支付业务。其中提到,将条码(二维码)应用于支付领域的有关技术,其终端的安全标准尚不明确,安全性尚存质疑,存在一定的支付风险隐患。这被很多业内人士质疑为是由于支付宝侵蚀了银联线下收单市场的利益。

然而,现在根据行业内“法不禁则行”的定律,各公司在私下里仍在偷偷进行二维码支付业务。目前,二维码支付主要分成 4 方力量在主导。

首先,是支付宝公司主导的“付款码”方式,它已经在全国 15 000 多家便利店和超市,还有像银泰百货这样的商场布置开来。其支付流程如图 3 所示。

经过实践分析,手机支付宝中的付款码信息只是一个数字序列,并无任何其他信息。它应用的是信息安全技术中的数字口令技术,原理为:手机支付宝客户端和支付宝服务器各自能产生数字序列,产生方法是前一串数字经过一个特定的单项函数后会产生后一串数字。手机支付宝中的数字序列和服务器的数字序列刚开始是相同状态,当手机产生新的数字串并传到服务器时,服务器也依次产生出对应的数字串,这样就能进行身份认证。如果服务器产生了一定数量的序列,却没有与客户端发送过来的对应,则会认证失败,手机客户端需要和服务器重新同步。

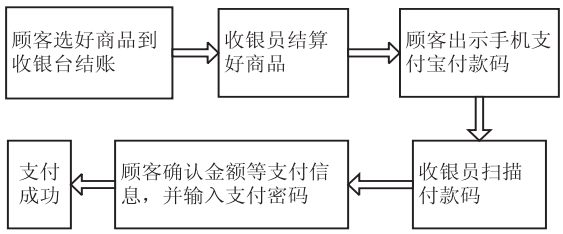


图 3　支付宝付款码支付流程

付款码支付过程具体的信息流为:收银员结算好商品,在结算电脑上产生交易商品信息,产生交易数字序列号;顾客点击付款码,手机支付宝产生付款码,即一个与该支付宝账户对应的数字序列号;收银员用扫描枪扫描付款码,扫描枪解析付款码信息,并传输到支付宝数据库中,验证与该序列号对应的支付宝账户,如果账户余额足够,则发送支付请求确认信息到顾客的手机支付宝;用户在手机支付宝弹出的请求确认支付框中输入支付密码确认支付,如果密码正确则交易成功;收银机打印交易凭条。

其次,微信在“微信支付”中推出一个新模块“刷卡”。微信的“刷卡”类似于支付宝的“付款码”,两者的支付过程和支付形式几乎一样。两者都是互联网巨头,凭借在移动端巨大的用户数发力,其影响力巨大。但是由于两者存在竞争关系,互相屏蔽了对方的二维 QR 码,这让有些商家在做二维码推广时,不得不制作双份二维码,增加了推广成本和麻烦。

再者,是以银行为代表的一方。银行和自己的特约商户合作,特约商户生成只对应于该行的二维码,而顾客只能用该行的移动客户端才能扫描解码。很多银行都推出自己的二维码,各家二维码不能相互识别,不易大规模推广开来。这里介绍中信银行推出的“异度支付”的支付过程:

(1)安装中信银行手机客户端。

(2)在客户端绑定一个中信银行账户。

(3)结账时,售货员在二维码终端机输入金额,二维码终端机产生支付二维码。

(4)顾客用手机客户端扫描二维码终端机上的二维码。

(5)扫描成功,手机客户端得到交易信息。

(6)用户确认交易信息,并输入密码确认。

(7)交易成功。

最后一方不可忽视的力量就是银联。在二维码推出以前,线下 POS 收单市场的费用是发卡行:收单行:银联按 7∶2∶1 的比例分配。当支付宝的二维码支付

推出到市场上以后,各方只需要在支付宝有一个结算账户,那么交易时的资金结算完全在支付宝体系内进行。银联被架空了,它的那一份收单结算费用就消失了。所以银联迫不及待要应对这种挑战,银联的策略是推出手机客户端二维码支付插件,该插件可以产生属于银联标准的二维码,并且可以扫描属于银联标准的二维码,然后将该插件整合到各家银行的手机客户端中。通过这种方法,银联在二维码支付中会要求银行进行手续费率的分成,仍旧可以谋取利益。另一方面,这种方法产生统一标准的二维码,各家银行客户端都可以扫描该二维码,有利于推广和方便用户使用。当然以后也有可能银联推出自己的手机二维码客户端软件,人们在一个客户端上可以绑定很多银行卡,在支付时只需要选择一张银行卡,然后客户端就产生对应银行账户的二维码[7]。

## 3 QR 码在应用中的安全问题

目前,二维码应用中存在很多安全问题,文献[8-9]有一些介绍。文中综合现存的安全问题和攻击方法,将其分为 4 类进行讨论。

### 3.1 物理攻击

物理攻击可以用笔涂改已有二维码,使用户扫描后定位到已被挂马控制的网站。其具体做法是,首先解析出原有正常二维码的信息,列举许多已被控制的与原二维码中网址相近的网址。然后按照原二维码的编码格式将这些相近网址进行编码,并与原二维码进行对照,选取与原二维码最相近的一个新生成的二维码,然后通过计算,涂改原二维码一部分像素单位,使用户扫描涂改后的二维码被纠错定位到有问题的网址。该方法比较笨拙,实现耗时费力,只能对一些特定二维码进行攻击。

### 3.2 扫描攻击

二维码在许多场合的本质是将用户定位到一个网址,而许多用户根本无法分辨该网址是否安全。因此,结合在计算机上基于网页攻击的方法,可以通过二维码,将用户定位到钓鱼网站,传播恶意 APP,甚至进行 SQL 注入,跨站脚本攻击,等等。例如,有报道的扫二维码支付宝钱包被盗事件,大多数情况其流程如下:

用户扫描二维码→程序识别结果为网址链接→程序询问是否打开→用户打开链接后自动下载恶意程序→下载完成→弹出 APP 安装界面并询问用户是否安装→用户选择安装→APP 安装完成→点击 APP 图标启动→手机中毒[10]。

之后木马病毒运行在用户手机中,读取手机号码并将其发送到木马制作者那里,木马制作者用该手机号登录支付宝网站并选择忘记密码。支付宝将验证码发送到用户手机,而用户手机中的木马比短信系统先拦截验证码短信,将其发给木马制作者,然后删除短信。在修改完支付密码后,木马制作者就可以对用户支付宝账户资金进行转账盗取,而用户却完全不知道。

### 3.3 隐私泄露

大多数二维码是明文编码的,为像上面提到的物理攻击提供了可能。铁道部在最初将二维码应用于火车票防伪时,并没有做好加密措施,从而产生了隐私泄露问题。此外,在进行支付宝二维码支付实验时发现,支付宝的“付款码”支持离线支付,当你开启小额免密码支付时,手机端产生付款码,在不需要联网的情况下,被扫描枪一扫就能扣款。

根据前面已经讲述过的原理可知,支付宝付款码序列码只是由手机客户端产生,而非联网后通过后台数据库产生,如果手机客户端的信息加密不当,非常容易造成信息泄露。有可能被黑客逆向后,找到生成付款码数字序列的方法[11]。

### 3.4 身份认证

由于二维码没有身份验证机制,用户无法鉴别一个二维码的真伪,这在一定程度上让一部分用户对二维码望而却步。另一方面,这也为基于二维码的一些攻击提供了土壤[12]。

## 4 QR 码安全问题的应对

信息技术中对安全性的要求在二维码应用中主要体现在 4 个方面:

(1)可认证性:对二维码来源是可以确认的。

(2)保密性:隐私的信息不能被非相关人员不法获得。

(3)完整性:确保二维码消息不被修改,如果遭到了修改,是可以被验证发现的。

(4)不可否认性:消息的发布者不能否认它发布的二维码。

根据安全性要求和上一节列举的二维码应用中的问题,基本的解决思路主要有两方面:对二维码内容进行加密和提供认证机制。

如果单纯的只对二维码进行加密,即对要编码的信息先加密,然后再将加密后的密文进行编码[13]。但是加密系统时常面临密钥更改的问题,如果不能方便进行整个系统的密钥更改,是不行的。加密手段在有些场合可以解决问题,比如火车票,因为火车票只在进出站时需要扫描,扫描解密密钥可在检票系统比较方便的同步或者更新。但是在其他场合,比如银行的二维码,它在加密后,就只能被自家的客户端解密。

身份认证,在电脑上已经有比较成熟的应用,如成熟的 PKI 体系。但是手机的计算能力有限,无法达到

RSA 加解密和证书认证的要求。然而,二维码的认证可以借鉴 WAP 中的 WPKI 密钥体系[14]。WPKI 是为无线环境中的应用提供密钥和证书管理,它采用 PKI 中简化的证书格式,并用加密能力更强但是对计算能力要求低很多的 ECC 公钥算法。

在国内,如果银联可以和支付宝,各银行联合起来,推出统一格式的二维码,并推出类似 PKI 体系的身份认证机制,二维码的应用将迎来一个新的春天。

此外,还有云扫描技术可以提高二维码在使用中的安全性。以往的扫描上网过程是:

(1)用户用手机客户端扫描二维码。

(2)手机客户端解析出二维码中的网址,并显示网址信息(有些客户端不显示网址,而直接连接)。

(3)用户点击网址。

(4)浏览器打开网址并连接。

现在电脑浏览器上都有云扫描过程,当你输入一个网址后,浏览器首先会先将网址与数据库比对,如果是一个挂马网站,浏览器就会提醒用户该网站危险,是否确认打开[15]。在手机客户端扫描二维码的过程中,也可以借鉴这一做法。客户端解析出网址后不会马上打开,而是先联网与后台数据库比对扫描,然后再提示用户操作。当然,要求联网可能会带来使用不便,在不要求联网的情况下可以使用离线数据库比对,这样也能大大提高安全性。

## 5　结束语

当前正处于移动互联时代,二维 QR 码由于优点众多而被广泛使用,给人们的生活带来了诸多益处,但也伴随许多安全隐患。随着手机计算能力的不断提升和人们对安全性的不断要求,相信在不久的将来至少在国内会形成比较统一的编码标准和身份认证以及加密体系。到那时,二维码将发挥更强大的作用。

**参考文献:**


[1]　Gao J Z, Prakash L, Jagatesan R. Understanding 2D-barcode technology and applications in m-commerce-design and implementation of a 2D barcode processing solution[C]//International computer software and applications conference. [s. l.]: IEEE, 2007: 49-56.

[2]　Li H. Benchmarking the use of QR code in mobile promotion [J]. Journal of Advertising Research, 2012(3): 102-117.

[3]　黄　宇. 二维码在移动电子商务中的应用[J]. 中国新通信, 2006(5): 78-80.

[4]　GB/T 18284-2000 快速响应矩阵码[S]. 北京:国家质量技术监督局, 2000.

[5]　潘继财. 二维条码技术及应用浅析[J]. 商场现代化, 2009(9): 118-120.

[6]　韩　韦. 手机二维码应用及安全性分析[J]. 信息与电脑:理论版, 2012(7): 19-20.

[7]　Lee Y S, Kim N H, Lim H, et al. Online banking authentication system using mobile-OTP with QR-code[C]//5th international conference on computer sciences and convergence information technology. [s. l.]: IEEE, 2010: 644-648.

[8]　林佳华,杨　永,任　伟. QR 二维码的攻击方法与防御措施[J]. 信息网络安全, 2013(5): 29-32.

[9]　Kieseberg P, Leithner M, Mulazzani M, et al. QR code security [C]//Proceedings of the 8th international conference on advances in mobile computing and multimedia. [s. l.]: ACM, 2010: 430-435.

[10]　栾　宇,李洪祚. 移动恶意软件治理关键技术研究[J]. 邮电设计技术, 2013(6): 52-55.

[11]　Gao J, Kulkarni V, Ranavat H, et al. A 2D barcode-based mobile payment system[C]//Third international conference on multimedia and ubiquitous engineering. [s. l.]: IEEE, 2009: 320-329.

[12]　Liao K C, Lee W H. A novel user authentication scheme based on QR-code[J]. Journal of Networks, 2010(8): 937-941.

[13]　付利莉. DES 算法在二维条码数据加密中的应用[J]. 石油化工高等学校学报, 2005, 18(2): 80-82.

[14]　冯　韵. 移动支付中身份认证分析与研究[J]. 信息通信, 2012(3): 107-109.

[15]　邸洪波,于绍辉,苏吉成. 网站安全扫描产品的分析与比较[J]. 信息网络安全, 2014(9): 180-183.