Science Discovery
2017; 5(5): 321-326
http://www.sciencepublishinggroup.com/j/sd
doi: 10.11648/j.sd.20170505.14
ISSN: 2331-0642 (Print); ISSN: 2331-0650 (Online)

The Reserch of Network User Account Security Problems and Solutions

Wang Chen, Li Jianbei, Li Shucheng, Wang Yinhui

Academy of Agriculture and Forestry, Yin Chuan, China

Email address:
Elanor2001@126.com (Wang Chen)

To cite this article:
Wang Chen, Li Jianbei, Li Shucheng, Wang Yinhui. The Reserch of Network User Account Security Problems and Solutions. *Science Discovery.* Vol. 5, No. 5, 2017, pp. 321-326. doi: 10.11648/j.sd.20170505.14

Received: June 15, 2017; **Accepted**: July 7, 2017; **Published**: August 4, 2017

Abstract: To improve the network service market, improve the information monitoring and filtering mechanism, to strengthen a sense of prevent and identify consciousness, using the security technology to protect the user's account. Proposed involving various types account detailed feasible safety protection scheme. Network user account security problems can be divided into account Settings, loopholes in management rules, improper operation and malicious steal four aspects are analyzed. At the same time, this paper also reveals the network account password security policy.

Keywords: Account Security, Binding, Security Policy

网络用户帐号安全问题及解决方案研究

王琛，李剑蓓，李述成，王银惠

农林科学院农业科技信息研究所，银川市，中国

邮箱
Elanor2001@126.com（王琛）

摘要：为完善网络服务市场、完善信息监测与过滤机制、加强用户防范与鉴别意识，利用技术手段保护用户的帐户安全。本文提出了涉及各种类型帐号的详实可行的安全保护方案。将网络用户帐户安全问题分为帐号设置、管理漏洞、操作不当及恶意盗取四个方面进行了分析，同时揭示了网络帐号密码设置的安全策略。

关键词：帐户安全，绑定，安全策略

1．引言

随着中国Internet网络的发展，网络购物、网络游戏、网络通讯交流越来越多地占据人们的生活空间。但随之而来的用户虚拟财产安全、信息安全、数据安全形势变得复杂难控。由于Wifi是一种共享媒介，更容易受到恶意攻击。例如通过身份验证泛洪攻击、evil twin. access point (AP) / Honeypot。此外，还存在某些用户大量占用无线带宽而导致其他用户可用带宽减少的问题；据中国网游产业报告显示[1]，2006年中国网络游戏市场的规模为65.4亿元人民币，增长率为73.5%，游戏用户总量为3112万。在如此巨大的游戏市场中，帐户安全状况却不容乐观，计算机病毒导致的虚拟装备被盗事件日趋严重。仅以2006年9月在全国范围内爆发的熊猫烧香病毒为例，作案人李俊通过盗取用户的网络游戏帐号，将虚拟装备转手卖出，在短短三个月中共获利145149元，让数以万计的游戏用户辛苦得来的装备一夜之间不翼而飞；现在随着微博用户数量激增与影响力的不断扩大，微博钓鱼、微博侵犯隐私、微博引发的群体性事件以及编写发布微博病毒等微博违法犯罪现象比较

突出；[1]中国互联网协会发布《中国网民权益保护调查报告》显示，2014年网民因为网络诈骗、垃圾信息、个人信息泄露等侵权现象导致的损失达到1433.6亿元。报告统计显示，有近80%的网民手机号遭到过泄露，并有50%以上的网民因手机号泄露而受到影响。病毒集团针对网购的欺诈手法也在花样翻新，钓鱼网站、网购木马、盗号木马让网购人群防不胜防，即使是一些资深的互联网用户也有可能掉入骗子的陷阱，淘宝店铺是实名认证，支付宝被木马劫持的话，帐号和密码是用户的唯一标识。一旦因为病毒等原因被其他人获得，用户的财产将面临严重的威胁。[2]2015年谢瑾在《网络用户账号密码安全问题调查》一文中发布了针对用户账号安全问题历时3年的测试分析成果，内容包括互联网主要网站的账号注册、登录以及认证的传输、存储及泄密的主要技术原因。[3]2016年冯涛在《基于属性加密的云存储隐私保护机制研究》以典型的云存储体系结构为研究对象，从数据拥有者、云服务器、授权机构、用户以及用户撤销机制5个方面对云存储系统的隐私保护机制进行了研究，通过分析比较发现，云存储系统中的隐私保护问题主要可以分为系统参与者的身份隐私问题、敏感属性信息泄露问题、云存储系统敏感内容信息泄露问题。[4]2017年毕晓迪在《一种基于隐私偏好的二次匿名位置隐私保护方法》一文中针对基于位置的服务带来的用户位置隐私暴露问题，提出了基于差分隐私的匿名位置生成算法，在保护用户位置隐私的同时确保获取精确的位置服务。因此，利用技术手段保护用户的帐户安全，对完善网络服务市场、提高运营商服务水平是十分必要的。为有效打击犯罪，应完善信息监测与过滤机制，加强防范与鉴别意识。为防止隐私泄露，应加强帐号安全和信息管理。

2．用户帐户安全问题现状

[5]目前，访问控制的权限设置采用的技术方法主要有三种，一是采用数字签名技术控制资源受限的传感器节点；二是用小权限法限制用户只能访问某些路径上的数据三是对访问节点的用户进行隐私保护，利用盲签名技术的DP2AC访问控制协议。但这三种技术方案又各有利弊，还有待进一步完善。

市场研究机构国际日前发布《中国第三方网络支付安全调研报告》，首次综合行业数据及大量的用户问卷和电话调查结果。[5]调研数据显示，目前在网民面临的各类安全问题中，“账户密码被盗”和“遭遇木马钓鱼”造成资金损失的占比分别达到33.9%和24%，成为网民的头号大敌。犯罪分子使用虚假身份盗用网络用户信息进行作案，因此犯罪行为隐蔽性很强，易于销毁证据，如电信诈骗、敲诈勒索、绑架、暴力讨债等违法犯罪活动。同时各类犯罪类型相互勾结交织，形成犯罪网络和利益链条，造成更加巨大的社会危害。

当公民发现泄露个人身份、散布个人隐私等侵害其合法权益的网络信息，或者受到商业性电子信息侵扰的，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止。任何组织和个人对窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为，有权向有关主管部门举报、控告；接到举报、控告的部门应当依法及时处理。被侵权人可以依法提起诉讼。这从法规上对网络用户的个人信息进行了保护。

2.1．账号设置的用户安全问题

网络本身只是攻击系统的一个渠道，最严重的问题是用户自身系统的安全问题，而解决这个问题比保护网络本身更困难。安全问题中一种是用户弱口令问题。网络里的很多用户喜欢使用简单数字、字母序列，个人生日、姓名信息这类极其简单的密码(口令)，结果导致邮箱被盗用、电脑被入侵。这是因为黑客手中都有一份密码字典，里面有几十万条常用密码，黑客可以通过密码字典很轻松的猜测出这类用户的密码。所以没有经过精心设计的密码，在网上使用一段时间后，基本100%会被破解，进而导致账户被盗用、系统被恶意攻击者攻破。还有一种比较常见的安全问题是，恶意攻击者在攻破用户系统后，把用户电脑作为傀儡机，或者利用用户电脑建立钓鱼网站。此外，现在的黑客攻击呈现暴力攻击事件越来越少的趋势。这是因为，暴力性攻击事件没有利益可以获取，而现在绝大多数攻击都具有经济利益目的，比如盗取网银、QQ、网游等的账号密码，攻击社交网站发起欺诈攻击。所以，现在的黑客攻击更注重隐藏性。

[5]中国软件评测中心联合多家权威机构，抽取了门户、邮箱、电子商务、招聘等9类100个网站，对在网站中使用的各类用途的用户口令处理进行安全性测评。测评结果令人担忧。100个网站中仅有8个网站对用户口令做了安全性处理，实施了安全防护，有59个网站使用户口令直接暴露无遗，在传输网络以及服务器端可以任意侦听，更有85个网站的用户口令能够批量获取原文。有很多用户为了使用和记忆的便利，在不同网站注册时习惯采用统一的帐号和密码，不难想见，一旦某一网站的信息泄密，用户在其它网站上的信息必然存在连带式风险。

据了解，中国软件评测中心将依据国家标准，面向网站等相关企业开展《个人信息保护管理体系认证》服务。中国软件评测中心副主任高炽扬建议，尽快建立个人信息保护体系，加强相关企业在技术和管理体系上对个人信息的保护力度，营造健康的互联网环境。同时，中国软件评测中心正在依据国家标准，面向网站等相关企业开展《个人信息保护管理体系认证》服务。

2.2．管理漏洞的帐号安全问题

注册帐号几乎是每一个网络用户都使用过的，要或真或假地填一些上传表格，从而在一个空间里有了一个身份也拥有了一些权限。但大多数人却忽视了在被赋予权力的同时，用户也要相应地履行一些义务，即要承担个人信息被公开，虚拟或实际的钱物受损失的风险。[6]据雷锋网报道，官方微博内突然会出现莫名信息，修改密码后仍然可见恶意信息。新浪微博企业客服回复“帐号疑似被盗，建议立即锁定。”可是锁定后雷锋网却无法登录，问题仍未解决。此事最终以新浪冻结雷锋网官方微博而收场。

在实际的使用中，这种情况已是寻常事——登录后进入别人帐号，而且发送微博显示在他人账号上；微博被恶意刷屏，莫名其妙的关注了很多人等等。不少用户质疑，到底为何会这么多帐号遭泄露？又是如何泄露的？即时通讯体系存在什么系统漏洞？对此，资深安全顾问张百川接受速途网采访表示，新浪微博就存在这系统漏洞，这种漏洞从本身上来说并不会导致帐号混乱，但是如果被恶意利用就会存在A端无故进入B端，B端信息显示在C端这样的情况。目前，网银和手机银行的安全已经引发业内关注，尤其是移动支付的兴起，越来越多的人开始使用移动银行，最新数据显示，中国手机网民已达5.27亿。XSS即跨站脚本攻击，攻击分成两类，一类是来自内部的攻击，主要指的是利用程序自身的漏洞；另一类则是来自外部的攻击，主要指自己构造XSS跨站漏洞网页或者寻找非目标机以外的有跨站漏洞的网页。黑客可以通过此漏洞，对用户进行“钓鱼”、偷密码，并且可以看到用户账号余额。因此作为用户账号的管理方，有责任提供全方位的信息安全服务，构建稳定可靠的网络或网络安全域之间信息的出入口，并且能根据安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。

2.3．操作不当用户安全问题

一些用户在注册时不注意阅读相关的协议，因此对有可能会面临的问题未能引起重视。重复申请注册、密码丢失、保存不当，在公共场所电脑上使用后没有及时清除记录等情况十分普遍。见下图：

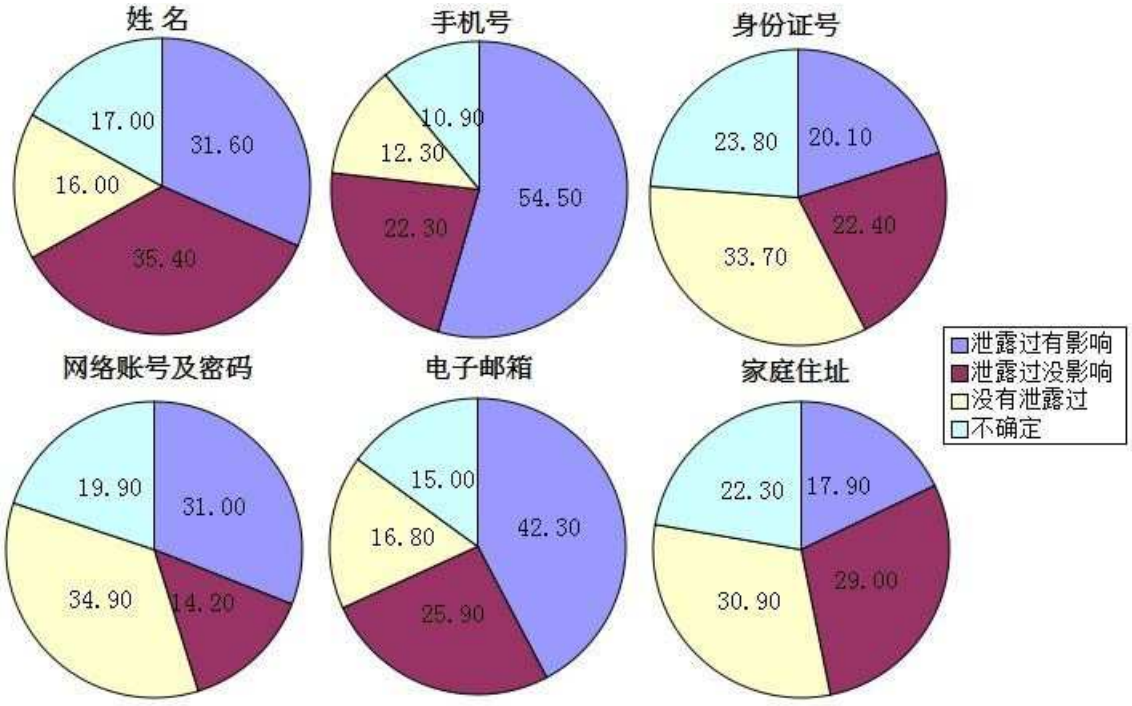

图1 2013-2014个人信息泄露侵权现象及影响。

向公民宣称可以监控他人聊天记录、手机短信甚至监听电话等。还有一些人员利用工作便利，对外出卖用户信息。人民网开展了一次有关个人信息泄露的调查，结果显示，90%的网友曾遭遇个人信息被泄露；有94%的网友认为，当前个人信息泄露问题非常严重。但由于买方与卖方多通过互联网联系，互相不认识，因此没有具体的受害人，犯罪行为和损害结果极难被察觉。不法分子通过倒卖公民个人信息牟取暴利，致使公民的个人隐私和财产安全受到前所未有的威胁。

2.4．恶意盗取的账号安全问题

在百度上输入“聊天记录”等字样时，会有诸如“QQ聊天记录查看器”、“微信聊天记录查看器”、“QQ聊天监控软件”、“远程监控聊天记录”、“如何查询聊天记录”等内容的信息。一些犯罪分子在网上或者以电话形式向公民宣称可以监控他人聊天记录、手机短信甚至监听电话等。还有一些人员利用工作便利，对外出卖用户信息。人民网开展了一次有关个人信息泄露的调查，结果显示，90%的网友曾遭遇个人信息被泄露；有94%的网友认为，当前个人信息泄露问题非常严重。但由于买方与卖方多通过互联网联系，互相不认识，因此没有具体的受害人，犯罪行为和损害结果极难被察觉。不法分子通过倒卖公民个人信息牟取暴利，致使公民的个人隐私和财产安全受到前所未有的威胁。

2.5．基于云计算的虚拟存储系统的安全问题

随着网络存储技术的逐渐发展成熟，云计算的虚拟存储系统被广泛的运用，但是要维持其长久的发展必须从其薄弱环节进行加强，保证数据存储的安全可靠性。[6]一旦

云计算中虚拟存储系统的用户账号被非授权访问，会对用户以及其存储的数据造成一定程度的危害，使数据在访问、存储、传输的过程中出现意外，导致数据被损坏，更甚者出现云系统崩溃的问题。

3．用户安全解决方案

3.1．帐号安全保护方案

随着网络的快速发展，多种网络，包括移动通信网络、车载网、无线局域网等，都可以提供无线接入服务，极大地方便了人们的生活。但是，每个接入点能够覆盖的范围是有限度的，因此需要通过一套合理的移动用户身份认证协议来为用户提供一种无缝对接服务。[7]通常来说，用户认证协议中包含的三个实体分别是：移动节点（MN）、接入点（APx）以及认证服务器（AS）。

对于用户认证系统的设计通常需要注意两方面的因素：一是计算效率，因为要维持移动节点的连续性，用户认证系统的计算过程需要快速且高效。另一方面就是注重安全和隐私问题。用户比较注重其身份、位置或者漫游路线等个人隐私问题遭到泄露，然而有很多公司对这些信息非常感兴趣。但是当前移动网络切换协议基本建立在假设所有的AP都是真实可信的，显然这是很危险的事情。综合分析现有的用户认证体系，在移动用户认证方面的工作还有待加强，相关保密措施还需继续研究。基于智能卡的密码认证技术能够有效地防止对密码的随意篡改，而且较为方便地管理这些密码文件，因此成为当前用户认证和建立会话秘钥比较简单且有效的一种方式。

一般情况下，为了评判基于智能拉的用户认证方案是否安全，主要假设的条件如下：（1）攻击者能够对用户、本地代理以及外地代理之间的通信信道进行随意的篡改、删除、插入等操作。（2）攻击者可能会提取用户的密码，也有可能获取的是智能卡的密码，但基本不可能同时获得这两个密码。但是就这两者比较而言，获取或者破坏智能卡的密码相对来说更为容易。目前可以主要通过研究基于智能卡的认证技术来提高整个移动网络的防御能力。帐号安全保护是提供服务方向服务使用方提供的一项关于帐号的安全保护措施。常见保护有：密保绑定、密码保护卡绑定、手机绑定、电话密保、邮箱绑定、IP地址绑定、身份证绑定、彩信密保、视频绑定等等。

3.1.1．密保绑定

密保采用的是动态口令防盗。优点是动态口令就算刚刚被人看去了密码和口令，但过不了一会口令就会变；缺点是电子产品寿命不够长。首次推出密保绑定业务的是盛大公司出品的盛大密保;[8]后期推出密保绑定业务的是网易公司出品的网易将军令，样式与盛大密保相差无几；其他还有使用该项业务的还有久游令牌。

3.1.2．密码保护卡绑定

密保卡采用的是固定口令防盗。优点是如魔兽世界采取的免费密保卡，随心换；缺点是万一卡弄丢了就无能为力了。

3.1.3．手机绑定

该方式一般来讲为选填项目。最常见的是腾迅公司出品的腾迅QQ（初期称作OICQ）。[15]一般该业务开通以后，作为密码找回的一项保护措施来用，方法是网页申请或发送短信，通过审核后新的密码由提供服务方发送到使用者手机上。一般与身份证绑定业务共同使用。

3.1.4．电话密保

该方式使用电话作为找回密码的媒介。

3.1.5．邮箱绑定

该方式使用电子邮箱作为找回密码的媒介。基本上凡是有申请帐号的页面都会提供该项目的填写。

3.1.6．IP地址绑定

该方式常用于电子商务或网上银行交易的漫游认证技术中。[7]这种保护方案需要满足几点要求：（1）获取服务器认证信息。（2）外地服务器可获取用户在本地服务器的认证信息。（3）外地服务器具有获取漫游用户是否无效的权限。（4）外地服务器和用户之间建立一个仅有双方知晓的随机会话秘钥。（5）用户信息仅有其本地服务器知晓，对其他任何服务器或个人完全匿名。（6）用户位置和信息的不可追踪。除了用户及其本地服务器之外的任何人都没有获得用户使用过或待使用的协议的权限。目前研究人员提出了许多这方面的认证协议，但是都还没能够完全实现上述六点要求。

3.1.7．身份证绑定

此方式应用广泛，可以说申请帐号的基本填写项目。网络游戏中使用该项目作为防沉迷系统的判断依据。在网吧中作为防止违法犯罪事件和判定犯罪嫌疑人的依据，也兼作密码找回使用。

3.1.8．彩信密保

[16]类似于手机绑定业务，因为使用的媒介同为手机，只是手机绑定密码找会采用的是短信息发送，该业务采用的是彩信发送，一般用来发送图片格式的密码保护卡。

3.1.9．视频绑定

与身份证绑定业务类似，多用于证明当事人身份，可以提高使用者本人的真实度。

3.1.10．身份证认定

上传身份证复印件，以确定真实身份，防止盗用。

3.2．帐号密码设置策略是用户安全基础的核心

如果丧失了密码，与帐号相关的基本安全机制和模式就没有了保障。为了设置一个配套的强固的密码，就需要用户在账号策略设置里拥有更多相关的选项。

3.2.1．密码复杂度一定要高

一个强固的密码至于要有大写字母、小写字母、数字、非字母数字的字符（如标点符号）中的三个内容。

3.2.2．密码保护都应该上齐

不使用普通的个人信息（如生日日期）；密码里不含有重复的字母或数字；至少使用八个字符。

3.2.3．尽量采用屏幕键盘

业内95%的木马都是利用的键盘记录，也就是说木马只能记录你键盘的输入信息（除了上下左右F1 F2 F3 F4等）。有很多系统有屏幕键盘，诸如一些专业的网上炒股系统。几乎所有木马都盗不走屏幕键的内容。因为他是用鼠标点的，木马只能记录鼠标按下、抬起，但不知道它点的什么，所以尽量用屏幕键盘这是最有效的方法。

3.2.4．U盾（移动数字证书）

当用户尝试进行网上交易时，银行会发送由时间字串，地址字串，交易信息字串，防重放攻击字串组合在一起进行加密后得到的字串A，[8]U盾根据个人证书对字串A进行不可逆运算得到字串B，并将字串B发送给银行，银行端也同时进行该不可逆运算，如果银行运算结果和你的运算结果一致便认为你合法，交易便可以完成，如果不一致便认为你不合法，交易便会失败。并且银行每次都会发不同的防重放字串（随机字串）和时间字串，[8]所以当一次交易完成后，刚发出的B字串便不再有效。到目前为止，理论上U盾是绝对安全的（理论上发生伪造概率大约为2的80次方分之一）。

3.2.5．加强社交网站中的安全建设

社交网站要想有一定的安全性能，就需要进一步优化社交网络中的软件，让用户在使用社交网站和软件的过程中，能够抵御病毒和木马的攻击，最大程度上降低病毒的影响。此外，用户在使用的初期也可以通过网络进行安全排查，相互加好友的过程中，通过检测对用户的信息进行检查，能够降低社交网站的漏洞。[9]如果在检测的过程中，发现了脚本错误，这就代表出现了恶意的攻击，需要网站能够进行排查并在检测漏洞的过程中，进行修复，保证网民可以在良好的网络氛围中交流。网民在使用社交网站的时候，也要自觉维护网络安排问题，一旦发现了任何不好的现象，就需要上报，确保自己处于安全性能良好的社交网络之中。

3.2.6．加强手机中无线通信网络安全的保护

人们开始越来越接受无线网络，[10]也有越来越多的人开始使用手机无线通信网络，这在生活中得到了很大的普及，越来越多的安全问题也开始凸现出来。手机无线通讯的安全问题也需要得到保护，比如现阶段网民大多使用安卓或者苹果自带的系统，这成为社会上的主流。但是手机上的这些系统都有第三方的应用空间，虽然能够进一步丰富手机的使用功能，[11]但是第三方服务器也需要对用户的身份进行验证，以及收集用户的信息，在以上的每一个过程中都会产生问题。用户在填写信息的过程中，需要对系统有所保护，以免出现信息泄露，此外，需要对系统进行必要的检测，一旦出现了安全问题，能够及时进行调节和修复，保证信息得到保护，增强手机无线通信的安全使用。

3.2.7．加强宏观调控，减少垃圾信息

针对目前的社交网络安全问题，相关部门并没有出台健全的管理方式和制度，因此相关部门还是需要加强管理工作，出台合理的制度，防止出现恶意信息传播以及用户的隐私被入侵，[12]一旦出现这样的人或者事件，可以给予严格的处分和解决。专业的制度可以改善社交网络的安全问题，例如BBS软件，就可以出台专项的解决方案，包含基本的管理规范和市场准则等等。对于社交网络上的社交软件，还需要有健全的内容，要对其加强审核，保证不良信息可以被过滤。社交网络还可以从监管方面出发，让社交网络的安全管理朝着良好的方向发展。

4．结论

在之前相当长的一段时间里，网络安全倾向于解决防病毒、防攻击这些具体问题随着互联网本身发展到了一定阶段，现在网络安全更强调的是网络整体秩序，只有保障网络整体秩序，[13]网络安全问题才能彻底解决。如果仅仅是专注于某一方面问题的话，往往是治标不治本。现在人们对于互联网的安全问题投入很大，而且几乎每个人都装有杀毒软件，但人们反倒愈发没有安全感，甚至连个人信息这样私人的资料都无法维护，这是为什么？究其根本原因是整个网络没有秩序，所以互联网安全在未来最重要的方面是建立有效规范的网络秩序，或者是建立起有效的信任机制，让用户生活在一个可信任的互联网环境中，而不应该是全民皆兵。可以说，目前互联网还处于初级阶段，当建立起了有序的互联网环境时，安全问题才能从根本上得到解决。总之，[14]网络在不断发展的过程中，有利也有弊，需要国家相关部门、企业、用户共同努力，营造良好的社交网络平台，净化网络安全，为人们生活质量的提升做出努力。

致谢

本文为一般项目《枸杞质量安全溯源系统研发与应用》（编号：NKYZ-16-1103）；《基于RFID技术的科研设备管理E平台开发》（编号：NKYJ-16-02）；《物联网技术在枸杞精准种植管理与质量溯源中的示范应用》 的阶段性成果之一。

参考文献

[1] 王欣，社交网络安全问题及其解决方案，《科技资讯》，2017(1)。

[2] 年谢瑾，网络用户账号密码安全问题调查，2015。

[3] 冯涛，基于属性加密的云存储隐私保护机制研究，2016。

[4] 毕晓迪，一种基于隐私偏好的二次匿名位置隐私保护方法，2017。

[5] 庹继光，网络信息保护决定对网络反腐的损益探析，《新闻大学》，2014(5)。

[6] 孙金青，我们该如何依法保护个人信息，《人民邮电》，2013(2)。

[7] 君君，当聊天记录只值70元时《信息安全与通信保密》，2013(3)。

[8] 于冲，侵犯公民个人信息犯罪的司法困境及其解决，《青海社会科学》，2013(5)。

[9] 刘延峰，公民信息保护迫在眉睫，《吉林人大》，2014(4)。

[10] 法律博客，《网络（http://blog.chinacou）》，2016。

[11] 国际，《传媒评论》，2014。

[12] 朱光磊，基于云计算的虚拟存储系统方案及安全研究，《电脑知识与技术》，2017(4)。

[13] 冯涛；殷潇雨，基于属性加密的云存储隐私保护机制研究，《网络与信息安全学报》，2016(7)。

[14] 刘兴云，大数据驱动的透明政府：前景与边界，《广州公共管理评论》，2015(11)。

[15] 韩莉；秦丽华，测试技术对网站中服务器端质量保证研究，《煤炭技术》，2013(10)。

[16] 张保富(导师：梁艳春)，综合征管数据监控系统的设计与开发，《吉林大学硕士论文》，2012(6)。