热烈庆祝 浙江省十二届人大五次会议 浙江省政协十一届五次会议 隆重召开

透视移动互联网络安全问题

—嘉兴市图书馆—

浙江省公共图书馆信息服务联盟

目 录

一、移动互联网概念 4
二、社会各界关注移动互联网安全....4
高层看台....5
专家视点....6
外媒聚焦....6
三、移动互联网安全的现状和问题....8
移动互联网安全问题日益凸显....8
移动互联网安全面临的挑战....9
移动互联网主要安全问题....9
四、加强移动互联网安全的举措....12
落实移动互联网审核制度，加强移动互联网监督....12
应用提供商应加强移动应用软件的安全防护意识....12
相关部门和企业制定并实施相关技术规范和标准....12
行业联合共同防御....12
借力技术....13
五、各省市针对移动互联网安全的尝试....14
上海： 率先发布移动互联网安全标准....14
广东：警方检测移动互联网应用安全 通报 20 款 APP 15
浙江：中国移动创新产品“天盾”等点亮互联网之光....15
安徽：国家级移动互联网安全测评中心落户合肥....16

免责声明:

浙江“两会”专题信息产品由浙江省公共图书馆信息服务联盟各成员单位联合编辑。信息内容采自公开的报纸、图书、期刊、数据库资源以及各大主流网站，每份专题我们都准确标明来源和出处，摘选信息内容的真实性、准确性和合法性由发布单位负责。

本期专题由嘉兴市图书馆编辑，如您需要更为详细的内容及跟踪报道，请与该馆联络。

一、移动互联网概念

移动互联网是指互联网的技术、平台、商业模式和应用与移动通信技术结合并实践的活动的总称。“移动互联网是以移动网络作为接入网络的互联网及服务，包括 3 个要素： 移动终端、移动网络和应用服务。”（来源：中国工业和信息化部电信研究院，移动互联网白皮书（ 2011 年） ）

在简单的移动互联网模式下，用户使用移动智能终端，通过将传统移动通信网络（ 包括 2G/3G/4G 网络） 或者通过无线通信网络作为接入网络，来访问传统互联网中提供的各类能够提供满足其个性化服务需求的可移动、可定制的应用（来源：孙其博.移动互联网安全综述.无线电通信技术[J]，2016（02）：1-8.）

移动智能终端具有终端智能化、服务个性化等特征，更使得安全与隐私保护成为了移动互联网所必须解决的一大紧迫问题。与传统终端不同，移动智能终端与生俱来的用户紧密耦合性决定了其信息的敏感性，而其具有的移动特性又对于信息安全的保护提出了更高的要求。（来源：信息科学，2015）

二、社会各界关注移动互联网安全

据通付盾移动应用监测平台的数据显示，2016 年第二季度移动恶意 APP 的数量超过 2 万个，移动应用的高位漏洞超过 300 万个。（来源：人民政协报 2016 -9 -27 第 006 版）

高层看台

习近平（中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长）:

2016年4月19日上午，习近平在主持召开网络安全和信息化工作座谈会时提出：“要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。”（来源：学习中国，2016-10-12）

2014年2月27日，习近平在中央网络安全和信息化领导小组第一次会议上强调：“中央网络安全和信息化领导小组要发挥集中统一领导作用，统筹协调各个领域的网络安全和信息化重大问题，制定实施国家网络安全和信息化发展战略、宏观规划和重大政策，不断增强安全保障能力。”（来源：中国新闻网，2016-12-20）

李克强（中国国务院总理）:

李克强在政府工作报告中提出，“制定‘互联网+’行动计划，推动移动互联网、云计算、大数据、物联网等与现代制造业结合，促进电子商务、工业互联网和互联网金融健康发展。”（来源：中国青年网，2015-08-06）

在2015年8月19日的常务会议上，李克强强调：互联网等行业政府既要‘扶持’，为大数据产业创造一个健康发展的环境，又要‘引导’、‘规范’，保障信息安全。”（来源：人民网 2015-08-20）

刘云山（中共中央政治局常委、中央书记处书记、中央网络安全和信息化领导小组副组长）:

在2016年9月19日国家网络安全宣传周开幕式上，刘云山强调：坚持网络安全和网络发展同步推进，网络安全和网络发展相辅相成，安全是发展的前提，发展是安全的保障。要把新发展理念贯穿到互联网建设各方面；要把增强全民网络安全意识作为一项基础性工作来抓，大力普及网络安全知识，加强网络安全教育，推动形成全社会重视网络安全的良好氛围。（来源：人民网 2016-09-20）

专家视点

马化腾（腾讯公司董事会主席兼首席执行官）:

开放安全技术和能力，守护网民上网安全是腾讯的企业社会责任。（来源：央广网 2016-10-13）

周鸿祎（360 公司创始人、董事长兼 CEO）:

“对付网络安全行之有效的方法，就是把每个网络用户动员起来，打一场网络安全的全民战争。”

柴洪峰（银联执行副总裁、中国工程院院士）:

随着我国信息技术在金融应用领域的进步，银行卡产业发展速度很快，银联交易量和发卡量已成为世界第一，安全方面也从磁条卡上升到 IC 卡，从 IC 卡上升到移动支付。“现在银联和中国电信、中国移动、中国联通三大移动通信公司均有合作。”“网络安全永远在路上，我们要联合起来打一场网络安全之战。”（来源：中青在线 2016-09-19）

杨树桢（国家网信办政策法规局局长、中国网络空间研究院院长）:

一方面要发挥移动互联网的驱动引领作用；另一方面，需强化移动应用程序及其分发平台的监督管理，从而营造良好的网络生态，使移动网络空间更加清朗。（来源：中国新闻出版广电报 2016 -7-12 第 007 版）

外媒聚焦

外媒：移动设备用户应关注的 10 大安全问题

（1）移动应用并不安全

来自安全公司 MetaIntell 的最新数据显示，在排名前 500 的 Android 应用中，高达 92%的应用存在安全隐患，并不存在绝对安全的移动平台。

（2）关注黑客的动向

英国杀毒软件厂商 Sophos 在 2013 年发布的《年度安全报告》显示，Android 已经超过 Windows 成为全球最让黑客“青睐”的平台，同时还有报告显示，iOS 是目前黑客数量增速最快的移动平台。

（3）通信是黑客攻击的主要目标

通信已经成为全球各地黑客们的主要攻击目标。短信是黑客们最常用的侵入移动设备盗取信息的方式，他们大多通过诱骗手机用户在电子邮件中点击恶意链接的方法来对设备发动攻击。

（4）窃取企业数据

IBM 旗下的移动设备管理公司 Fiberlink 最近表示，在被企业拉入“黑名单”的应用中，排在前面的都是包括 DropBox 和谷歌 Drive 在内的云端存储服务。

（5）硬件的安全

对于智能手机和平板电脑来说，由于其移动性很强，所以很容易被窃取。

（6）越狱会增加设备的风险

遭到黑客攻击的 iOS 设备中大部分都是越狱设备，因为越狱之后允许用户在设备上安装并运行未经验证的应用。

（7）企业的生物识别安全问题

生物识别技术也是企业用户不得不提防的领域，例如指纹识别模块和虹膜扫描仪等生物识别设备有助于提升设备的安全系数，但是这对于企业来说可能会是一场噩梦。

（8）恶意软件越来越多

知名安全厂商 McAfee 上个月发布报告称，2013 年针对移动设备的恶意软件较 2012 年增长了 33%，目前的情况下，移动端的恶意软件还没有减缓的趋势。

（9）电子商务中潜在的危险

随着电子商务的蓬勃发展，这些黑客转而将目光放在了智能手机和平板等移动设备上，所以当你是使用移动设备进行网络交易时，一定要慎重。

（10）政府的监听

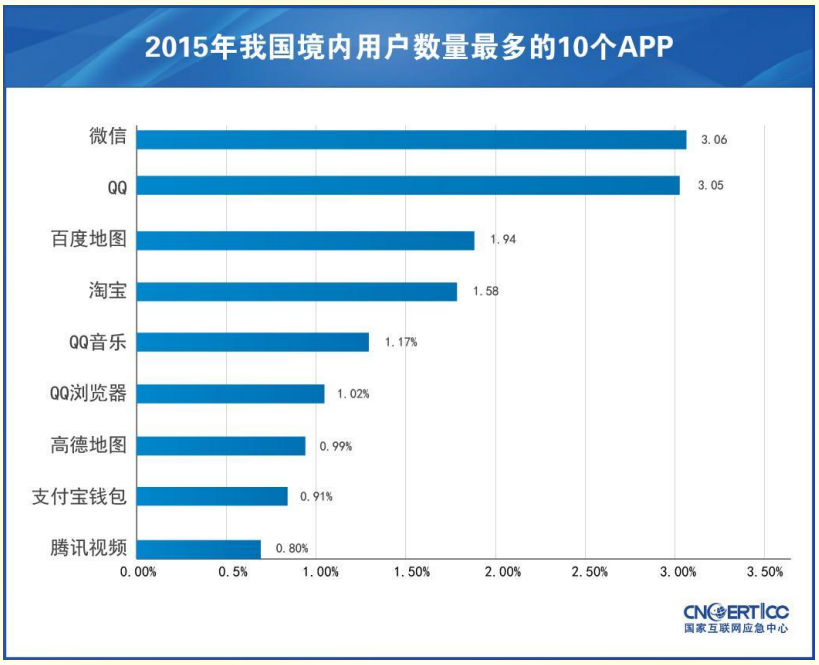
2014 年 1 月的一份报告指出，某第三方移动广告网络允许 NSA 访问用户的数据，并能获得这些用户的全部信息。所以，对于手机用户来说，还需要时刻提防来自政府方面的监听。（来源：微媒体 2014）

三、移动互联网安全的现状和问题

移动互联网安全问题日益凸显

根据国家统计局最新一次统计结果显示，全国人口数量为 13.7 亿，可见全国约有 56.9%的人口在使用移动互联网，如何保护 7.8 亿手机网民的上网安全问题值得高度关注。

从智能手机 APP 使用情况看，2015 年境内手机网民使用量最多的前三个 APP 是微信、QQ 和百度地图。移动互联网已逐渐融入网民的娱乐、购物、社交等日常生活中。2015 年境内手机网民上网时最常使用的 10 个 APP 如图所示。



2015 年我国境内用户数量最多的 10 个 APP（来源:《中国移动互联网发展状况及其安全报告（2016）》）

据某研究机构的报告显示，2016 年全球移动互联网用户总数将达到 20 亿人，占互联网用户数 62.5%。然而，随之而来的安全风险也开始成倍增长。伪基站诈骗、盗窃用户信息等问题已经成为当前手机用户的“家常便饭”。央视 3.15 晚会已经连续三年关注信息安全问题，但依然不断有用户网购被骗、手机被吸费等恶意行为发生。

据国家信息安全测评中心移动互联网安全技术实验室主任王嘉捷透露，2015 年底中国移动互联网使用人数已达到了 7.9 亿人，预

计到 2018 年将达到 8.9 亿人。该组织对全网做过一个漏洞威胁分析，在全国 50 多万个 APP 中有将近 50%的 APP 存在高危漏洞。从行业上来讲，游戏娱乐行业和生活服务类行业的 APP 在恶意 APP 中占比较大，类似社交、医疗、移动支付理财等领域也是问题集中地。（来源：人民政协报，2016 -9 -27 第 006 版）

随着应用商店安全管理制度的逐渐完善，恶意传播源也正在从应用商店延展到云盘、网盘等其他应用平台上，移动网络安全问题日益复杂和多变。

移动互联网安全面临的挑战

通付盾公司总裁王梅表示，目前移动应用安全主要有四个方面的挑战：一是开放平台的问题，由于开放性导致它成为安全的重灾区；二是基础较差，普通的开发者大部分仍缺乏安全意识，很重视功能但在安全意识上并不强；三是问题多，包括病毒木马、假冒、内容违规等诸多问题；四是监管难度大，尤其是对恶意行为源头的挖掘，对传播的途径管控都面临很大的难题。

（来源：人民政协报，2016 -9 -27 第 006 版）

移动互联网主要安全问题

（1）移动智能终端层面临的安全问题

其一是非法内容传播；其二是恶意吸费；其三是用户隐私窃取；其四是移动终端病毒以及非法刷机导致的黑屏、系统崩溃等问题。（来源： 邮电设计技术，2013（10））

大量 APP 存在内容方面的问题。报告显示，有 75%的被核查 APP 存在涉黄问题，其中匿名社交类 APP 问题突出，包括用户发布色情信息、提供色情服务，发布色情图片、视频和文字等情况。2015 年，12321 举报中心共下架处置涉黄 APP235 款。移动网络攻击、诈骗、侵权的现象高发，利用移动互联网传播色情、暴力等有害信息的恶劣行径也大量存在。2015 年我国感染移动互联网恶意程序的境内用户高达 1.74 亿。12321 举报中心（网络不良与垃圾信息举报受理中心）称其在 2015 年共接到手机应用软件（APP）举报 727976 件

次，有效举报 200684 件次。被举报的 APP 大多涉及偷跑流量和恶意广告插件问题等网络安全问题。

（来源：人民邮电，2016-5 -30 第 005 版）

（2）网络层面临的安全问题分析

移动互联网具有的网络开放性、IP 化以及无线传输的特性，使安全成为其接入网以及核心网面对的关键性问题之一。但是受限于现有技术能力，移动互联网尚缺乏对隐藏在所传输信息中的恶意攻击进行识别与限制的能力。按照攻击的方式，移动互联网的网络面对的威胁方式有窃听、伪装、破坏完整性、拒绝服务、非授权访问服务、否认使用/提供、资源耗尽等。（来源： 通信技术，2013）

（3）应用层面临的安全问题

移动互联网带动了大批具有明显个性化特征，并且带有移动特色的创新型和融合型移动应用的快速发展。这类移动互联网应用一般都具有很强的信息安全敏感度，拥有如用户位置、通信录及交易密码等用户隐私信息。按照通行的分类方法，移动互联网应用面临的安全威胁（来源：保密科学技术，2014（3））主要包括 SQL 注入、分布式拒绝服务（DDOS）攻击、隐私敏感信息泄漏、移动支付安全威胁、恶意扣费、恶意商业广告传播、业务盗用、业务冒名使用、业务滥用、违法信息及不良信息等。在内容安全方面，还面临着非法、有害和垃圾信息的大量传播，严重污染了信息环境。

有 10%被核查 APP 存在篡改手机号行为。通过篡改用户手机号，在他人手机上显示任意号码，能让人对各类电信诈骗犯罪虚构的事实信以为真，是通信信息诈骗的重要环节。12321 举报中心截至 2015 年年底共下架处置改号软件 34 款。还有 8%被核查 APP 存在滥发短信息以及恶意发送大量短信给他人行为。2015 年 12321 举报中心共下架处置短信轰炸类 APP25 款。（来源：人民邮电 2016 -5 -30 第 005 版）

2015 年上半年涉及用户资金安全的资费消耗和恶意扣费类病毒

类型占比超过 80%，对用户的安全威胁最大；隐私类病毒占比仅为 1.80%，但攻击方式更加多元化，如与短信相结合的“相册”木马病毒通过钓鱼、诱骗、欺诈的方式窃取用户姓名、身份证号、银行卡号、登录账号密码等重要的隐私信息，严重威胁用户财产安全。（来源：移动终端白皮书（2015 年），2015）

（4）移动互联网应用平台软硬件漏洞

此外，移动互联网应用平台由于软硬件存在的漏洞，也极易受到来自外界的攻击。

截至 2015 年，网络不良与垃圾信息举报受理中心共接到来自移动应用软件举报 72.8 万件。根据上海市信息安全测评认证中心数据显示，截至今年 8 月，测评中心接受送检的 31 款移动应用软件中，共发现安全漏洞 302 个，逾七成为中高风险漏洞，其中数据泄露类漏洞达 25%。“近半的安全漏洞发生在软件设计阶段。”（来源：上海法治报 2016 -9 -21 第 A02 版）

（5）应用提供商缺乏移动应用软件的安全防护意识

而另一方面，由于进行安全防护将会给应用平台带来附加的检测支出，且不会带来额外收入，导致应用提供商通常缺乏为用户提供安全防护的意愿。

王嘉捷表示，在移动安全方面从产业的角度来说，在产业开发运行上一些开发者的安全意识还比较淡薄，造成很多应用程序安全无保障。（来源：人民政协报 2016-9-27 第 006 版）

在许传朝看来，由于各方防范意识较薄弱，骗子通过各种钓鱼软件、恶意 APP 等获得的信息更加全面，目前已形成了集团化产业化运作。（来源：人民政协报 2016-9-27 第 006 版）

（6）移动 APP 市场审核不严，缺乏监管

王嘉捷还表示审核不严也是一个问题。目前国内有 300 多家应用市场，不仅应用发布门槛较低，大量恶意应用还提供了便捷服务，导致恶意 APP 市场野蛮生长；此外，对应用市场也缺乏相应有效的监管和有力的措施。（来源：人民政协报 2016-9-27 第 006 版）

四、加强移动互联网安全的举措

落实移动互联网审核制度，加强移动互联网监督

在应用市场审核上，相关部门要逐渐提高审核标准。可以通过引入第三方或者专业国家级的测评机构进行统一的把关，提高准入门槛。作为行业的监管部门要制定相应的严格市场监管措施，提高监管力度。（来源：人民政协报，2016 -9 -27 第 006 版）

应用提供商应加强移动应用软件的安全防护意识

移动终端开发者应具备并加强应用软件的安全防护意识，保障移动终端用户使用的安全性，这样才能从本质上赢得用户的青睐。各个企业可以针对重大行业制定安全保护解决方案。

相关部门和企业制定并实施相关技术规范和标准

上海市信息安全测评认证中心主任蒋力群：“移动应用软件的相关技术规范非常必要。”（来源：上海法治报，2016-9 -21 第 A02 版）

刘振飞（阿里巴巴首席风险官）：阿里巴巴正在牵头制定相关的国际标准、国家标准和行业标准，希望以此来推动整个行业、整个生态安全的提升。

行业联合共同防御

腾讯推动以技术对抗为先行，行业联合共同防御的“腾讯模式”，基于腾讯海量大数据能力，在打击电信网络诈骗、打击网络谣言、提供人群热力图服务等方面，取得了不错的成绩。（来源：央广网 2016-10-13）

蚂蚁金服安全部：“生物识别技术将是未来移动支付的发展方向，具有唯一、稳定和难以复制的特点，能有效提高支付的安全性，减少密码泄漏的风险。”（来源：中青在线 2016-09-19）

2016 年 12 月 6 日，由中国消费者报社与北京等全国 37 省市区消协（消委会、消保委），联合全国移动互联网安全测评中心共同开展

的“严防信息泄露 强化风险防范——构筑移动互联网应用安全防线全国行”活动在京启动，以加强移动互联网领域的消费教育和引导，强化消费者的风险防范意识，确保广大消费者的消费安全

借力技术

通过移动安全大数据应用为移动互联网保驾护航。

2016 年 9 月，武汉举行的网络安全博览会上大数据技术在防范和打击电信诈骗方面的应用吸引了众多目光。多家互联网科技企业展出了同公安部门联手在全国范围内检测、打击伪基站的监控系统，该系统。通过大数据分析，“测算”出伪基站的具体位置。用户客户端能够提供的数据信息越多，分析定位就会越精准。目前，公安部已向全国省级公安部门推广使用**伪基站实时监控系统**，目前全国 31 个省市已经全部开通。（来源：央视网 2016-09-22）

2016 年 10 月 12 日，第二届“全国大众创业万众创新活动周”现场，腾讯公司董事会主席兼首席执行官马化腾介绍：**腾讯推“守护者计划”，大数据反诈骗。**腾讯基于腾讯手机管家、电脑管家海量用户和全球最大安全云库的大数据分析能力，推出了两款大数据反诈骗产品——“鹰眼”智能反电话诈骗盒子和“麒麟”伪基站实时检测系统，分别与运营商、公安等开展合作，取得了良好的效果，切实为技术对抗黑产提供了大数据解决方案。（来源：双创周：李克强总理听取马

化腾介绍腾讯安全反诈骗模式 央广网 2016-10-13）

（马化腾介绍腾讯安全反诈骗能力和模式）

除了在行业上合作，腾讯的安全产品也在不断提升实用的安全能力。今年 9 月，腾讯手机管家为苹果开放的来电识别接口提供骚扰拦截技术支持，基于腾讯全球最大的骚扰诈骗电话号码库和独创的反诈骗核心技术。

移动互联网用户：加强安全防护意识，保护个人信息

中国互联网协会和国家互联网应急中心提示：**普通用户在平时使用移动互联网时，要谨慎识别伪基站短信和电话，尽量从官方渠道下载手机 APP，并且在安装软件前仔细阅读软件权限。**

五、各省市针对移动互联网安全的尝试

上海： 率先发布移动互联网安全标准

2016 年 9 月，上海率先发布移动互联网安全标准《移动互联网应用软件安全通用技术规范（试行）》，从技术安全和安全管理等方面，全面保护移动互联网用户个人敏感信息。

该规范从技术安全和安全管理两个方面，对移动互联网应用软件提出安全要求，具体包括：身份鉴别、逻辑安全、数据安全、外部防护、安全设计、安全开发、安全维护等 10 个部分。针对移动互联网用户身份证号、手机号等个人敏感信息的使用和保护，规范作出了严格要求。比如，规定要求，移动应用软件应该提供用户输入密码及敏感信息，诸如身份证号、手机号、邮箱、姓名等信息的即时防护功能，不被其他软件截获；敏感信息在输入完成后，应立即进行加密，内存中不应存在完整的敏感信息；通过公共网络传输时，应对敏感信息采取加密措施确保其保密性等。（来源：上海法治报 2016-9-21 第 A02 版）

广东：警方检测移动互联网应用安全 通报 20 款 APP

为规范 APP 市场管理、防范和打击违法 APP，促进移动互联网健康发展，自 2014 年 8 月起，广东省公安厅网警总队对省内重点 APP 市场进行安全检测和整治，督促 APP 商店安全严格落实安全技术措施，深入排查安全隐患和管理漏洞，全面清理违法有害软件。

2016 年 3 月起，为进一步净化广东移动互联网环境，省公安厅网警总队开通“违法 APP 曝光台”，通过广东网警微信公众号（微信号：gdgawj）、平安南粤网（www.gdga.gov.cn）、粤警民通 APP 三种渠道，定期向社会公开曝光传播违法有害信息、吸费、盗取公民个人隐私等侵害公民权益的 APP，提醒广大网民加强防范、及时卸载，确实保障网民隐私和财产安全。（来源：中国新闻网 2016-03-22 11：21：02）

浙江：中国移动创新产品“天盾”等点亮互联网之光

中国移动自 2014 年于浙江开始了“天盾”反欺诈系统的研发，力图建设国际改号诈骗电话的监控系统，通过基于“识别+研判+拦截”的骚扰诈骗电话集中治理方法实现诈骗号码准确、全面识别与处置。

中国移动利用大数据分析技术，首创了可对疑似诈骗行为识别、分析和处置的办法。

2016 年 8 月，浙江丽水青田一位市民接到一个电话，对方要求其把卡里钱转到自称是民警所提供的安全账户上。中国移动“天盾”反

欺诈系统通过智能分析程序成功抓取这一异常电话，从而及时制止了该市民的受骗行为，挽回损失近500万元。这就是中国移动“天盾”反欺诈系统取得的显著成效。（来源： 浙江在线 2016-11-16）

安徽：国家级移动互联网安全测评中心落户合肥

2015年，中国信息通信研究院与中国联通安徽分公司签约，在合肥高新区共建全国移动互联网安全测评中心，为国家级移动互联网安全测评中心。项目依托于安徽捷兴信息安全技术有限公司，将充分发挥中国信息通信研究院与中国联通安徽分公司在移动互联网、信息安全、应用测评、安全加固、渠道分发能力等方面的优势资源，面向移动互联网、物联网、未来网络等热点领域，通过建立移动互联网领域的应用安全监测平台、白名单应用发布平台与公共服务支撑平台，提供行业监控、软件测试、应用发布、行业支撑、资源共享、质量跟踪等专业化服务，打造专业从事移动互联网信息安全服务的国家级质量保障、风险评估与技术服务支撑的权威职能机构。（来源：安徽日报 2015-10-26 ）