浅析手机存在的安全隐患及防范对策

李忠伟
鲁东大学　云南省楚雄彝族自治州楚雄市　264000

[摘　要] 目前，随着科技的发展，移动通信和信息化的迅速发展，是智能手机最新的移动通信技术，智能手机之所以流行，是因为它不仅具有传统的手机通信功能，而且还具有传统的手机通信功能。人们使用智能手机下载应用程序通过互联网，可以很快并方便举行视频会议，移动办公室，网上商店，网络游戏，语音聊天等。

[关键词] 手机；存在安全隐患；防范对策

引言

智能手机的出现导致了我们生活中的质的变化，它成为一个工具来交换我们的工作，我们的生活百科全书，甚至我们的银行在手，这让我们知道世界的动态，直到我们离开家。只要我们可以使用智能手机，使我们方便快捷，危险逐渐逼近我们。最近，许多犯罪分子看到了我们对手机的依赖，并开始寻找从中获利的办法，例如窃取我们的信息，将其出售给有关的公司，从而偶尔骚扰垃圾信息，手机欺诈、个人过滤、更糟糕的是，通过在线交易偷钱以窃取我们的银行密码，为了使这些问题不影响我们的正常生活，解决移动电话安全问题已经成为我们大家的共同目标。我们必须面对。

1 Android 手机所存在的安全问题现状

随着科技的进步，智能手机处理器的处理速度越来越快，手机的容量也越来越大。因此，用户对手机厂商所持有的软件感到不满足。可是，手机的系统变得不稳定，手机的危险性增大。同时，用户自己安装了的软件的安全性也不能预测。因为一部分非法分子有可能通过手机软件取得用户的隐私。目前，移动电话的应用范围广泛，主要分为社会应用、制图导航、因特网支付、生活费、电话通信、搜索工具、照片美化、音频和视频转播、阅读等类别。

2 智能手机存在的安全隐患

2.1 明文传输成为信息泄露的“窃听器”

移动电话的通信通常是明确的，可以在任何时间、任何地点、任何人截获，甚至可以成为隐藏的“麦克风”，但条件是必须有相应的接收设备。无线电通讯，他们有一个通道，这也是一个开放的电磁空间。现在频道攻击主要有两种方法。一个是信号接收，机密使用相应的设备，直接捕捉空中的移动电话通信信号，通过数据处理恢复声音和数据。另一个是基站的欺诈。非法分子在手机和基站之间设立假基站，同时欺骗双方的信赖，接收和转发双方的信息。不仅仅是盗取情报的目的，还可以篡改手机的通信内容。有人会认为，窃听不会被窃听，直到他们打电话。实际上，没有，在等待状态下，手机可能会破坏保密性。一些进口的移动电话已被引入一个特殊的程序，具有秘密电话的功能，一些恶意软件的移动电话也可以进行远程控制，无论是等待还是等待。关闭手机，将其转换成聊天状态，无需调用，无屏显示，传递周围的声音，在这种情况下，手机周围的任何声音都可能被窃听。

2.2 操作系统存在许多安全漏洞

智能电话使用的是开放的操作系统，虽然这些系统很容易使用，机器人操作系统的分裂问题大大降低了移动电话的运行速度，增加了恶意网络攻击的危险，ICOS 系统中有一个“后门”，泄漏后有泄漏的危险，以及一个漏洞。这些漏洞使操作系统成为海盗袭击的主要目标，在这方面，我国代表团支持秘书长的建议。针对智能电话操作系统中的漏洞，黑客开发和开发了一系列专门仪器或木马病毒，以攻击移动电话，破坏移动电话保护系统，通过不正当地扣除移动电话的费用，窃取商业秘密和个人隐私，这种病毒可以自动进入网络，移动电话在重新启动或点燃时可以启动，并开始进行破坏。

3 手机安全隐患防范对策

3.1 彻底删除不需要的信息

当用户从移动电话中删除或格式化信息时，该信息不会被删除，只是从主要的导航区域中删除信息，改变管理结构和标记为可用的。如果有新的信息，它可以被重写，但不覆盖，除非它是由于物理原因被破坏，但它仍然在存储和可以恢复。因此，当需要更换电话或处理相关信息时，可选择使用具有数据切碎能力的移动电话软件，或在改装移动电话时，重新储存大量无用数据，如电影录像带、垃圾文件，在电话存储器中，反复删除无效信息，重新填充电话空间，完全覆盖原始信息，增加数据的检索。

3.2 不断完善应用软件的审核监管体系

关于移动电话应用程序的安全问题，各国应采取适当的法律政策和条例，包括对移动电话使用的保密要求，特别是严格控制资格，第三方智能移动电话应用程序或软件供应商的身份和服务质量，并尽可能确保其所提供的软件商店的现有资源是合法的，从根本上确保移动电话用户下载和使用的移动电话的通用程序是合法和正常的，并确保个人隐私权和信息安全

3.3 掌握安全防范常识

不要轻易回答，你收到陌生人的电话，短信，彩色信件，电子邮件，更不要点击额外的信息，如果有必要，请关掉手机，完全切断电源，以防病毒或木马被输入。不要把手机放在自动屏幕上，每次打开屏幕，都会输入密码设计要充分利用。

3.4 利用正规平台下载 App

智能手机用户下载应用程序时，应登录正式平台，避免从论坛等非正式平台下载。请不要使用来源不明的软件。请不要看坏页面。正规的手机经营者持续手机的维护，防止病毒对策程序的导入。安装应用程序时，请务必仔细查看软件所要求的权限列表，如果有敏感的权限请特别注意。如果软件要求提供与服务无关的地址簿、短信等权限，请阅读 App 并请求获得照相机访问权限，必须警惕是否有陷阱。

4 结语

在当今信息化时代，智能手机与人的生活是不可分割的，对人的生活有着巨大的影响。在提高人民生活质量方面的作用，然而，他们自己的安全问题也有违反保密性的危险。通过分析智能手机的发展和面临的安全问题，提出了切实可行的保护措施，加强智能手机的安全，减少了侵犯隐私权的可能性，并确保了用户的信息安全。

[参考文献]

[1] 姚培娟，张志利 .Andrid 智能手机安全问题和防护策略研究 [J]. 现代计算机（专业版），2015(1):69-72.

[2] 赵飞 . 智能手机泄密风险分析及安全保密技术方案 [J]. 电子技术与软件工程，2017(2):216.

[3] 李维华 . 智能手机风险分析与安全防护 [J]. 网络安全技术与应用，2015(9):79-80.

[4] 杨璞 . 智能手机泄密风险分析及安全保密技术解决方案研究 [J]. 网络安全技术与应用，2015(4):138-139.