智能手机连接涉密计算机的管控机制分析

● 邢 彬 何建波 余彦峰 张江雷 / 国家保密科技测评中心

【摘 要】本文详细介绍了安装iOS系统或Android系统智能手机连接Windows操作系统的表现形式和常见USB设备管控方法，分析了智能手机连接涉密计算机时，存在的安全风险和设备管控软件可能存在的不足，并从管理和技术两方面提出了管控建议。

【关键词】智能手机 涉密网络 设备管控 风险分析

1 引言

智能手机正快速地占领手机市场。美国独立民调机构皮尤研究中心（Pew Research Center）于2016年5月发布的报告显示，2016年中国智能手机普及率已达58%。移动互联网市场研究机构艾媒咨询（iiMedia Research）于2017年3月发布的报告显示，2016年全年中国手机市场出货量达5.6亿部，其中智能手机5.22亿部，占比93.2%。与传统手机相比，智能手机的处理速度更快、存储空间更大，还具有独立的操作系统，使人们的工作和生活变得更加便捷。

智能手机通过USB线缆连接计算机时，会呈现类似U盘的存储设备，不仅可以管理手机中的文件，还可以为手机充电。很多人认为，涉密计算机中的U盘管控系统能够起到有效的防御作用，通过USB接口连接手机不存在失泄密隐患。这种做法是否安全呢？本文将以安装iOS系统和Android系统的两种典型智能手机连接Windows XP和Windows 7两种常见的操作系统为例，讨论智能手机连接计算机的安全风险和管控机制。

2 智能手机连接协议和表现形式

2.1 安装iOS系统的手机

iOS系统是苹果公司以Darwin系统（UNIX系统的一个分支）为基础，为iPhone手机、iPad平板等移动设备开发的操作系统。由于iOS系统并不开源，目前市场上安装iOS系统的手机只有iPhone手机。下面讨论iPhone手机连接计算机时使用的协议和表现形式。

（1）通过PTP协议、MTP协议连接

计算机在未安装iPhone专用手机驱动时，操作系统会使用自带的驱动程序连接手机。其中，Windows XP会通过USBScan驱动程序、PTP协议（Picture Transfer Protocol，图片传输协议）

进行连接，Windows 7则通过MTP协议（Media Transfer Protocol，媒体传输协议）进行连接。此时iPhone手机会被识别为数字相机，用户仅能查看和下载手机相册中的图片，无法执行其他操作。

（2）通过专用设备驱动连接

苹果公司的官方手机管理软件iTunes中集成了iPhone手机专用驱动程序。在安装该软件后，Windows操作系统会将连接的iPhone手机识别为手机设备，通过iTunes软件，实现手机和计算机间双向的文件传输。如果手机开启“个人热点”并允许通过USB连接，计算机中还将添加类型为Apple Mobile Device Ethernet的网卡，此时计算机可通过手机数据网络访问互联网。表1是对iPhone手机连接计算机情况的总结。

2.2 安装Android系统的手机

Android系统是Google公司以Linux系统为基础，为移动便携设备开发的操作系统。Android系统是开源的，各厂商在遵循相关协议的基础上，对系统进行修改和二次开发，因此Android系统在智能手机、平板、机顶盒和其他智能终端中得到了广泛应用。下面讨论安装Android系统的手机连接计算机时使用的协议和表现形式。

（1）仅充电模式

将手机以“仅充电”模式连接计算机时，计算机通常能够识别手机型号，但用户无法查看手机中的文件，也无法向手机中写入文件。

（2）PTP模式

PTP模式在一些Android手机中被称为“传照片”模式。以该模式连接计算机时，Windows XP像连接iPhone手机一样，使用USBScan驱动程序和PTP协议，用户可使用系统自带的图片导入工具，查看和下载手机相册中的文件，但无法查看手机中的其他文件，也不能向手机中写入文件。Windows 7操作系统会使用MTP协议进行连接，用户使用系统中的文件管理器即可访问手机中的相册目录（如DCIM）、具有图片属性的目录（如Pictures），但无法访问其他目录。需要说明的是，Windows 7系统和Android手机间的MTP协议是双向的，用户不仅可以查看文件，还可以向上述目录中写入文件，包括非图片格式的文件。

（3）MTP模式

MTP模式在一些Android手机上也被称为“传文件”模式。在该模式下，Windows XP、Windows 7操作系统都需要使用MTP驱动程序与手机建立连接。Windows XP默认版本并没有

表1 iPhone手机连接计算机的情况

连接方法	操作系统	表现形式	功 能
未安装设备驱动	Windows XP	设备管理器：名称为Digital Still Camera的图像处理设备 我的电脑：名称为Apple iPhone的扫描仪和照相机设备	单向PTP协议，仅能查看手机中的相册，不能向手机中写入文件
	Windows 7	设备管理器：名称为Apple iPhone的便携设备 计算机：名称为Apple iPhone的便携设备	单向MTP协议，仅能查看手机中的相册，不能向手机中写入文件
iTunes（安装设备驱动）	Windows XP和Windows 7	设备管理器：名称为Apple Mobile Device USB Driver的通用串行总线控制器	具有较全面的设备操作功能，例如，查看相册、安装应用程序、在手机和计算机间上传下载文件、通过手机数据网络访问互联网

集成MTP驱动，但可通过将系统中的Windows Media Player播放软件，升级到10或更高版本来获得MTP驱动。这里使用的MTP协议也是双向的，用户可通过文件管理器，对手机内部存储和外置SD卡中的数据进行读写。

（4）U盘模式

有些Android手机支持U盘模式。以这种模式连接时，计算机中将出现可移动磁盘的盘符，用户可像操作U盘一样，读写手机内部存储模拟SD卡目录和外置SD卡中的数据。

（5）ADB模式

ADB（Android Debug Bridge，Android调试桥接）模式是为调试Android设备而设置的连接模式。以该模式进行连接，不仅需要Android手机设置中开启“开发者选项”并启用“USB调试”功能，还需要在Windows操作系统中安装ADB驱动程序。在连接建立后，用户通过命令行或第三方管理工具，不仅能够访问手机中的文件数据，还能够读取或修改手机联系人、通话记录等数据，安装或删除软件等。如果手机系统没有对root权限做出限制，那么ADB模式连接时，将能够以手机系统的最高权限进行操作，包括修改Android系统底层配置等危险操作。需要说明的是，在Android 4.0及以上版本操作系统的手机中，只有在手机弹出的对话框中选择“信任该计算机”后，才能建立有效连接。

（6）FastBoot模式

FastBoot模式和ADB模式有相似之处。这种模式的连接需要Android手机以FastBoot模式启动，并在计算机中安装BootLoader Interface驱动程序。在这种模式下，用户可通过FastBoot命令行或相关工具对手机进行管理操作，该模式主要用于手机刷机或还原出厂设置。

（7）USB网络共享模式

如果将Android手机通过USB线缆连接计算机，并在手机设置中开启“USB网络共享”功能时，计算机中将添加类型为“Remote NDIS based Internet Sharing Device”的网卡。Windows 7操作系统可自动安装该网卡的驱动程序，Windows XP操作系统虽默认不含该网卡的驱动，但可通过手动安装使该网卡变为可用状态。在USB网络共享模式建立后，计算机将可通过Android手机的数据网络访问互联网。

（8）其他模式

除上述Android原生操作系统所具有的连接模式之外，一些手机厂商还会根据需要设计一些特殊连接模式，例如，部分华为手机提供了HiSuite连接模式，该模式的文件传输等功能和MTP模式是相同的。表2是对Android手机连接计算机情况的总结。

Android手机能够同时以多种连接模式连接计算机。例如，当手机以仅充电模式连接计算机时，依然可同时通过ADB模式、USB网络共享模式进行连接。但部分连接模式存在互斥关系，例如，仅充电模式、PTP模式和MTP模式不能同时连接，FastBoot模式与其他模式也不能同时连接。

需要特别说明的是，由于Android操作系统是开源的，手机厂商可进行定制或修改，因此手机连接计算机时的实际表现形式和功能可能与表2存在差异。例如，小米、部分华为手机通过USB连接计算机时，会在计算机中增加光驱设备，光盘内容为手机说明文档或连接软件。表3列出了常见Android手机支持的连接模式。

3 USB设备管控原理

USB接口具有支持设备种类多、扩展灵活和即插即用等特点，已成为计算机中使用频率最高的外设接口之一。鼠标和键盘等人体工学设备、智能卡读卡器和KEY等认证设备、移动硬盘和U盘等存储设备及光驱、打印机、扫描仪、摄像头等设备，都可通过USB接口便捷地接入计算机。在涉密计算机中，禁用USB接口虽然能够很好地限制违规设备接入，但也会阻碍人体工学设备和认证设备的接入。为此，很多涉密计算机都通过安装设备管控软件进行安全防护。

表2 Android手机连接计算机的情况

连接方法	操作系统	表现形式	功 能
仅充电模式	Windows XP	设备管理器：名称为手机型号的便携设备 我的电脑：名称为手机型号的其他设备	无有效操作方式
	Windows 7	设备管理器：名称为手机型号的便携设备 计算机：名称为手机型号的便携设备	无有效操作方式
PTP模式	Windows XP	设备管理器：名称为手机型号的图像处理设备 我的电脑：名称为手机型号的扫描仪和照相机设备	PTP协议，在Windows XP操作系统默认应用程序支持的情况下，只能将手机相册中的文件导出到计算机中
	Windows 7	设备管理器：名称为手机型号的便携设备 计算机：名称为手机型号的便携设备	双向传输的MTP协议，只能看到手机中的相册和图片属性目录，可在计算机和手机间上传或下载文件
MTP模式	Windows XP	设备管理器：名称为手机型号的便携设备 我的电脑：名称为手机型号的其他设备	双向传输的MTP协议，可在计算机和手机间上传或下载文件，需安装Windows Media Player 10或更高版本
	Windows 7	设备管理器：名称为手机型号的便携设备 计算机：名称为手机型号的便携设备	双向传输的MTP协议，可在计算机和手机间上传或下载文件
U盘模式	Windows XP 和 Windows 7	设备管理器：名称为USB大容量存储设备的通用串行总线控制器 我的电脑/计算机：U盘或可移动存储设备	可在计算机和手机间上传或下载文件，通常只显示手机SD存储卡或模拟SD存储卡中的内容
ADB模式	Windows XP 和 Windows 7	设备管理器：名称为Android Composite ADB Interface的Android Phone设备	可在计算机中，通过adb命令行或第三方管理工具对手机进行任意读写操作
FastBoot模式	Windows XP 和 Windows 7	设备管理器：名称为Android BootLoader Interface的Android Phone设备	主要用于在计算机端对手机进行刷机或还原出厂设置等操作
USB网络共享模式	Windows XP 和 Windows 7	设备管理器：名称为Remote NDIS based Internet Sharing Device的网络适配器 控制面板中的网络连接：类型为Remote NDIS based Internet Sharing Device的网卡	可在计算机中，使用手机数据网络连接互联网

下面对USB设备栈结构和USB设备管控原理进行简单分析。

3.1 Windows操作系统USB设备栈结构

Windows操作系统中对USB设备访问操作是按照栈式结构进行的[1]，自下至上分别是主机控制器、集线器和客户设备，如图1所示。主机控制器最核心的功能是控制主机与各USB设备的通信，包括设备接入和拔出的事件响应、数据传输控制等；集线器用于挂载各USB设备和其他集线器，系统可通过集线器和设备的级联关系找到每一个设备；客户设备是呈现设备自身功能特征的部分，也是应用程序和用户实际使用的部分。对于手机等提供多种功能的USB设备，Windows先将其视为一个复合设备，然后再将每个功能视为独立的用户设备。

表3 Android手机支持的连接模式

手机型号	仅充电模式	MTP模式	PTP模式	U盘模式	ADB模式	FastBoot模式	USB网络共享模式	其他
红米	不支持	不支持	不支持	支持	支持	支持	不支持	-
小米3	不支持	支持	支持	不支持	支持	支持	支持	-
小米5	支持	支持	支持	不支持	支持	支持	支持	-
华为Mate 7	支持	支持	不支持	不支持	支持	支持	支持	HiSuite模式
Nobia	支持	支持	支持	不支持	支持	支持	支持	-

当USB设备接入计算机时，操作系统将按照标准通信协议与设备通信，获取设备类型编号、生产厂商编号（Vendor ID）、产品编号（Product ID）等信息。设备类型编号须遵守USB规范，例如，03h表示人体工学设备，08h表示大容量存储设备。生产厂商编号由USB组织统一分配，每个厂商的编号都是唯一的。产品编号则由各厂商自行制定。系统将通过这些信息，标识USB设备，查找和记录每个设备所使用的驱动程序。

设备栈中的每个组件都需要驱动程序的支持才能有效工作。USB控制器厂商会提供主机控制器和集线器的驱动程序。Windows操作系统不仅会集成常见的主机控制器和集线器驱动程序，还会集成鼠标和键盘等通用的客户设备驱动程序。如果Windows中没有默认可用的客户设备驱动程序，或希望使用设备的特殊功能，则需要用户安装由客户设备厂商提供的驱动程序。此外，Windows操作系统还提供了过滤器驱动接口。调用该接口的过滤器驱动程序可在原驱动程序执行前或执行结束后运行，实现改变原驱动程序执行参数或结果的目的。

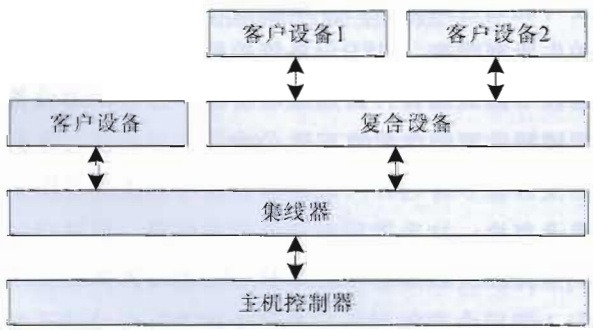

图1 Windows操作系统USB设备栈结构图

3.2 USB设备管控原理分析

USB设备管控系统有多种实现方法，常见方法包括：（1）限制驱动程序的加载；（2）通过过滤器驱动程序改变原有的驱动行为。一些简单的USB管控软件会使用方法（1），其主要原理是通过修改注册表、系统配置和驱动程序的信息文件等措施，使系统无法自动找到或加载适用的驱动程序，从而无法正常使用接入的USB设备，但这些措施无法受到有效保护，容易被破解或被绕过。方法（2）工作在驱动程序层面，改变原有驱动程序的行为，具有较好的管控能力和较高的安全性，是目前主流USB管控软件使用的方法。

通过方法（2）进行USB管控时，过滤器驱动程序工作的位置和方式决定管控能力。工作在底层的过滤器驱动程序能够获得底层USB设备的通信数据，包括设备类型编号和厂商编号等，但无法获取来自上层应用程序的语义信息。因此，底层过滤器驱动程序能够有效地对特定类型设备进行管控，例如，限制对大容量存储设备的读写访问等，但管控粒度依然较粗。工作在上层的过滤器驱动能够获取丰富的语义信息，包括访问设备的用户和进程信息等，具有细粒度的管控能力，但由于上层的驱动程序非常多，实现全面的设备管控也会存在一定困难。对于智能手机设备来说，USB组织未对智能手机设备分配专用的设备编号，通过底层

过滤器驱动程序难以直接禁用手机设备；而作为复合型设备，智能手机具有较多功能，且未来还可能会有更多功能，通过上层过滤器驱动程序进行管控也存在一定风险和挑战。

用户访问U盘以及通过MTP协议连接智能手机时涉及的协议和驱动程序如图2所示。虽然种访问在底层都涉及集线器驱动和主机控制器动，但上层使用的协议和驱动程序却并不相同传统U盘管控软件主要通过阻止加载USB存储动程序、阻止与大容量存储类设备通信等方法

图2　U盘和智能手机访问过程和可能的管控方法

制U盘的使用，但这些方法无法管控通过MTP协议连接的智能手机。

4 智能手机连接涉密计算机的安全风险和管控建议

从上述分析可以看出，智能手机连接计算机时会呈现多种设备属性，包括便携设备、大容量存储设备、网络设备等。虽然在部分模式下，计算机无法向手机传输数据，但由于手机能够同时以多种模式与计算机建立连接，设置不当依然可能会产生严重的失泄密隐患。如果仅通过安装U盘管控软件对大容量存储设备进行限制，智能手机依然可以使用MTP、PTP等便携设备的通信协议连接计算机，难以对智能手机进行有效管控。因此，必须从管理和技术上对智能手机连接涉密计算机的行为采取必要防范措施。

在管理方面，必须严格禁止智能手机通USB线缆连接涉密计算机；在技术方面，应当计算机系统中，安装管控方法更全面的USB设管控软件，在设备栈各层次进行监视，从系统置、驱动程序等多方面进行管控，及时阻断对机存储空间、访问手机数据网络等读写行为，强对智能手机等复合设备的管控能力。同时，着智能手机技术日新月异的发展，未来智能手还可能通过其他新的方式连接计算机，引发更的失泄密隐患。USB设备管控软件厂商需及时进技术发展趋势，研究应对措施，弥补USB设管控软件可能存在的不足。END

参考文献：

[1] Russinovich M,Solomon DA,Ionescu A.Windo Internals (6th edition).Redmond:Microsoft Pre 2012.