

打印机安全风险与防范解析

● 史 岗 李 姗 / 中国科学院信息工程研究所

随着我国信息化水平的不断提高，计算机外设类输出设备在信息系统中的地位越发重要，覆盖多种重要行业，包括党政军重要部门。

打印机虽然只是连接在计算机主机以外的外设设备之一，但由于其具有独立数据处理能力，能够和主机的交互进行数据传输，并具备一定的数据存储功能，已成为计算机系统中非常重要的组成部分，甚至可以影响整个计算机系统的运行。大家耳熟能详的例子就是海湾战争中，萨达姆的防空系统因为打印机内置的后门程序导致整个防空系统瘫痪，最终决定了战争的走向。因此，在信息技术迅猛发展、信息安全越来越重要的环境下，打印机的安全同样也需要高度重视。

一、打印机运行原理和机制

打印机所采用的技术可分为：分柱形、球形、喷墨式、热敏式、激光式、静电式、磁式、发光二极管式等。激光打印机目前应用较为广泛，本文将以其为例介绍打印机的运行原理和机制。激光打印机进行打印的主要过程为：充电—曝光—显影—转印—消电—定影—清洁[1]。激光打印机内部由机械部分及电子控制部分组成，是典型的机电一体化产品，电子控制部分通常被高度集成在打印机控制卡上，用来控制机械部分来完成整个打印工作。打印机的核心部分称为打印引擎。打印引擎包含以下5个主要部件[2,3]，其原理框图如图1所示。

◇激光扫描头（Laser Scan Unit，LSU），主要是将高低电平的数字信号转化为激光信号，让OPC（Organic Photoconductor）感光；

◇感光鼓（OPC Drum），是打印机的主要

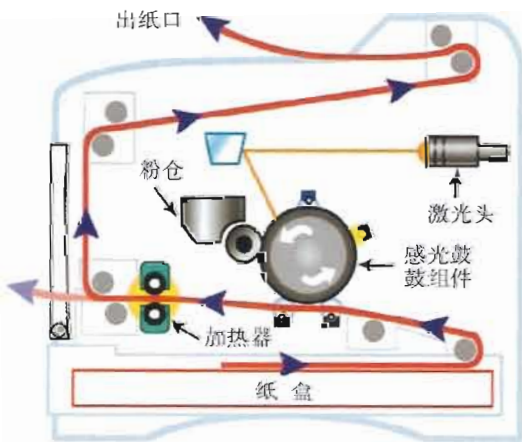

图1 打印引擎原理框图

成像部件，在特定波长的激光照射下，其表面电位发生变化，当其表面电位发生变化后，可吸附带电的碳粉；

◇马达，主要负责打印过程中纸张的输送；

◇定影单元，主要功能是对黏附到纸上的碳粉进行加热，使其融化并对其施加一定的压力，让其渗透并固化到纸张上；

◇激光碳粉盒，粉盒是主要的成像单元，其存储的碳粉是消耗品，用完后要重新更换。

除了以上部件外，打印引擎上还有一些电子电路控制单元。

◇电源板，因其控制大功能的定影器，与一般的电源板不同；

◇高压板，产生3000伏的高压直流电，用于成像的控制；

◇引擎控制板，主要控制走纸、卡纸检测、加热、LSU、高压等打印引擎的行为和动作，负责打印机内部机电一体化零部件的控制，如LSU、马达、定影单元、粉盒芯片、粉盒上（成像系统的高压）各种传感器等；

◇数据控制板，主要是负责接口（如USB/Network/Wi-Fi等）图像数据的处理，通常情况下，如果是一体机，该板也负责扫描引擎的控制、扫描图像的处理、复印流程的控制、复印画像的处理等；

◇面板，负责状态显示与参数设置。

打印任务需依靠打印机和PC端共同配合完成。打印系统的组成如图2所示。打印驱动程序是打印系统的核心，主要工作是将从应用程序中接收到的打印内容转换成打印机所能识别的由页面描述语言所描述的页面，通常是一些像素为单位的点阵位图图像，然后通过调用操作系统的底层接口将其通过PC端与打印机的连接接口传送到打印机上[4]。

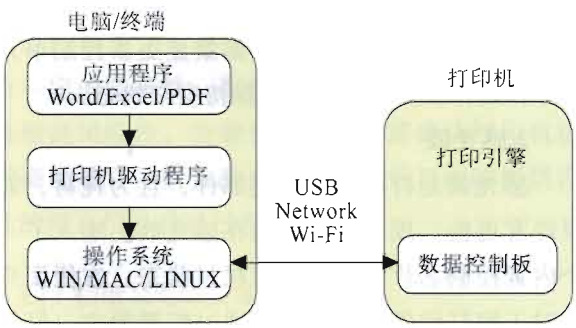

图2　打印系统组成图

二、风险漏洞与防范

（一）驱动

打印机的驱动包含两方面：驱动程序本身及PC端数据存储。

驱动程序是直接由打印机厂商提供的，且每台打印机都必须使用。由于驱动程序直接与操作系统交互，能够接触涉密计算机甚至通过非法调用操作系统内接口，从而获取涉密网络内的所有计算机信息，风险等级非常高。驱动程序可能存在的风险方式是被预埋木马等病毒，从而引发驱动非法截获打印内容，以及未经授权收集并转发PC端或与PC端相连的网络内与打印作业无关的内容。该风险可通过核验驱动程序是否具有国内公司的自主知识产权的方式来规避。

PC端数据存储是打印系统中重要的数据缓存，其中存有待打印或已打印未及时删除的数据，风险等级非常高。一些已被删除的包含打印内容的临时文件可能被间谍软件等恢复、复制、还原。打印过程中，文件或数据都是以明文方式存储的，多数采用标准打印语言，如PCL、PS，被间谍软件截获后，可通过专用的工具轻易打开获取原始信息，造成泄密风险。该风险可通过在驱动程序中增加部分模块来确保打印后及时删除相关文件并对缓存数据、文件采取非明文方式存储的方式进行防范。

（二）接口

打印机接口是打印机获取打印数据流的唯一通路。通常市场上打印机的接口依据连接媒介可分为两种：与PC端接口（包含间接接口如路由器转接接口）和部分可移动存储介质（如U盘

等）接口。第一类接口不仅有有线传输方式，还有多种无线传输方式，如Wi-Fi、蓝牙、红外等。第二类接口多为USB等供存储媒介直接插入的接口。

该接口为打印数据传输的必经之路，接口协议为明文传输方式且无设备管控、识别功能，故打印机接口为高风险等级的模块。打印机接口存在的风险主要包括4种：第一种，无线接口的存在导致涉密信息被间谍机构在外围窃取的风险；第二种，打印机与PC端采用的传输协议是明文传输方式，存在被网络内间谍软件非法破获涉密信息的风险；第三种，先行的PC端和打印机传输协议仅仅通过IP地址完成识别，存在被不法分子对安全打印机进行替换窃取涉密信息的风险；第四种，打印机机身上集成的可移动存储设备接口，存在被非法人员利用获得已窃取涉密信息或向涉密载体输入间谍软件的风险。

为了避免如上风险，首先，需要对打印机接口进行限制，涉密环境内的打印机应取消无线接口及可移动存储设备接口，用物理方式截断间谍程序的出入口；然后，将打印机和PC端的传输协议修改为非明文传输方式，即使涉密信息被窃取也很难破译出原始信息，为数据传输通路增添一层保障；最后，增加打印机和PC端之间的设备认证机制，确保每次打印任务发起后都是由已知安全的打印机完成，维护安全打印链路的完整性。

（三）打印机本体

打印机在数据通路中且需要对数据进行处理的部件包括：激光扫描头、感光鼓及电子控制单元中的引擎控制板和数据控制板。以上部件都存在被间谍软件攻击导致涉密信息泄露的可能。现在，部分打印机中引擎控制板和数据控制板两个电子控制单元已经合并为一个电子控制单元，叫作打印控制单元。这两个部件虽功能并不相同，但存在的风险漏洞是相似的，所以需要针对打印控制单元做风险分析。

1.打印机控制单元

打印机控制单元包含CPU、程序及独立存储空间。为了不断提高打印速度，打印控制单元内部存储在不断扩大。由于该单元能够直接接触到打印机的数据流，内部有能够独立完成程序的运行及数据存储的硬件平台，同时打印机内整个数据链都是明文传输，存在很高的风险。打印控制单元存在的主要风险包括4种：第一种，打印机控制单元内的控制程序可能隐藏部分非法指令和通信协议，主动向特定的接收设备或网络进行非法数据传输，或在输出介质上留下与原始打印作业无关的附加信息，造成泄密的风险；第二种，由于打印机控制单元的硬件上可能存在多余的硬件功能模块或者多余的板载存储空间，如CPU内部存储、设备内存储，能够非法存储打印内容；第三种，打印机控制单元内作业完成或错误恢复后，打印内部缓存中的内容未及时清除，给间谍程序提供了可乘之机；第四种，为了提高打印质量需要更新打印机控制单元内的程序，但未经授权的更新可能会给经过检验的安全的打印机重新引入第一种风险。

为了避免以上风险，需要经过以下4步确认：第一，确认打印机开发商的板载程序全部为自主开发且掌握源代码，能够证明不存在间谍模块；第二，由开发商提供主控电路板的PCB图、BOM单及存储模块的数据结构说明文件等，确认电路中不存在非法模块及冗余存储空间；第三，尽量选择国产自主可控的CPU且对CPU代码进行审查；第四，加入能够及时清除打印机缓存数据的控制程序，确保数据使用完毕后立即被清除；第五，从程序及设备管理两方面禁止更新控制单元程序，确保检测过的打印机保持安全状态。

2.感光鼓

感光鼓是打印机的关键部件，且为耗材，需要经常更换。现今的打印机在感光鼓上加入了一个内置控制芯片，能够体现耗材状态，方便用户随时了解打印机状态；能够通过配置粉盒、打印机的成像参数，提高打印品质。虽然感光鼓是数

据链路上的一环，但是仅能存储少量数据，所以风险性为中等。第一，由于感光鼓需要不断更换，所以很容易被改造后用于非法行为，比如加装非法小元件（如语音窃听器、无线发射模块等），或者内置一段引导程序，诱发隐藏在打印机控制单元中的隐藏模块以实现非法操作；第二，由于需要存储及运行程序，硒鼓内置芯片中也会有一定易失及非易失存储空间，可以保存非法数据，但数据量较少；第三，虽然硒鼓每次只能获得一页数据，但是由于机械原因，可能会存在部分残留影像被非法分子轻易获取的风险。

防范以上风险的措施包括如下3条：第一，硒鼓引入风险的主要来源是其需经常更换，所以需严格控制硒鼓的来源，采用经过国内安全认证机构认可的芯片作为硒鼓芯片，自主设计芯片控制程序，通过耗材与主机交互认证命令，使用只与主机配套的专用耗材，为了杜绝硒鼓内的附加部件，需确保硒鼓提供商具有硒鼓的全部电路的自主知识产权且经过详细审查；第二，硒鼓内置芯片的功能较单一配备的存储空间也非常有限，所以可通过多余装置的检测即可抵御相关风险；第三，打印完成或错误恢复时硒鼓内的残余信息需通过打印控制单元的配合进行清除。

3.激光扫描头

激光扫描头是在打印控制单元和硒鼓之间传递数据非常重要的模块，所有的数据都要经过激光扫描头发送给硒鼓。激光扫描头中的关键部件物理位置的安装有非常严格的要求，是直接影响成像的关键，所以激光扫描头通常都是一个被封装好的模块，再组合进入打印机中。由于封装具有一定的隐蔽性，存在隐藏非法电路的可能，具备较高风险性。为避免该风险，需确认打印机提供商能够自主研发激光扫描头，并且能够提供设计的所有信息且经过安全审查。

（四）物理及电磁安全

从整体角度分析打印机安全，其风险来自于以下2个方面：整机完整性及电磁安全。保证打印机的完整性能从根本上抵御由外来非法模块引入的风险，可通过机箱上锁等物理防护措施来保证打印机的完整性。

打印机中存在的电磁辐射可分为：处理器的辐射、通信线路的辐射、转换设备的辐射。打印机处理的信息能够通过特殊设备及截获的电磁波恢复出来，造成泄密风险。文献[5]对打印机的电磁防护做了一些探索，国家保密局也对涉密环境使用的设备的电磁辐射指标做出相关规定。

三、结语

打印机的安全风险来自于打印机与PC端组成的整个系统中所有与信息链相关的模块或组件。由于相关模块或组件的不透明，可能隐藏非法收集、传输涉密信息的风险因素。因此，实现打印技术的自主化和打印机软硬件模块的国产化对于打印机安全而言是至关重要的。只有实现整个打印系统内信息链上的软件、硬件模块自主化，并在关键模块中内嵌有效安全机制，才能解决打印机自身安全问题。同时辅以对打印机使用环境、元器件采购流程的安全管控，以及打印过程的安全审计，就能确保整个打印系统的安全，最终形成一个安全可靠的涉密信息处理环境。 END

参考文献：

[1] 田宏强,张军.激光打印机维修技能实训[M].北京:科学出版社,2011.

[2] 程鹏.激光打印机墨粉的鉴定方法研究[D].北京:国际关系学院,2012.

[3] 王楠.常用激光打印机打印文件特点的研究[D].上海:华东政法大学,2013.

[4] 蒋大奎.面向Windows的PCL6打印机驱动程序[D].广州:华南理工大,2007.

[5] 赵永昌.打印机的电磁兼容研究[D].上海:华东师范大学、2011.