打印机信息安全风险与防范措施研究

郭 磊 刘 博 崔中杰 / 国家保密科技测评中心

【摘 要】打印机作为常用的信息设备之一，在给我们工作和生活带来诸多便利的同时，由打印所产生的信息泄露等信息安全问题也日趋严峻。本文通过对打印机硬件、软件、通信和耗材等可能涉及信息泄露的风险点进行深入研究，总结了打印机的安全隐患，并提出了相应的防范措施，为提升国产打印机的信息安全防护性能，防范打印安全风险提供借鉴。

【关键词】打印机 信息安全 风险点 防范措施

1 引言

打印机是一种将计算机处理结果输出至物理介质上的电子设备[1]，它已经成为现代办公系统中不可或缺的环节之一。但在打印机工作过程中，有可能处理用户隐私、商业秘密甚至国家秘密，这些信息一旦被泄露，将对用户利益、企业业绩甚至国家安全造成不可估量的损失[2]。根据国外信息安全权威机构的统计，重要信息系统网络信息泄露的主要途径有3种[3]，分别是网络邮件、移动存储和打印。其中，移动存储泄密和电子邮件泄密已经被管理员给予足够重视。但是打印机信息安全问题一般很少被关注，这也是重要信息系统网络安全体系中较为薄弱的环节之一。

由打印机引发的恶性泄密事件已经屡见不鲜，为适应新形势对打印机信息安全防护提出的新要求，提升打印机产品的安全防护性能，杜绝重要信息系统网络中打印作业的信息泄露隐患，本文针对打印机工作过程中涉及的硬件、软件、接口、通信和耗材等可能导致信息泄露的风险点进行分析和研究，总结了打印机的信息安全风险，并提出了相应的防范措施。

2 打印机安全风险分析

打印机通常由硬件电路、光学成像结构，固件、驱动程序、审计管理系统和机械结构等部件组成[3]。在打印机工作过程中，任何一个环节都可能存在信息泄露的风险。

2.1 打印数据传输泄密风险

用户启动打印作业后，打印数据通过传输介质从用户端下发到打印机，过程如图1所示。

在这一过程中存在以下3个泄密风险点。

第一，通信接口泄密。现代打印机为满足多样化的用户需求，一般会配备丰富的通信接口，这些接口可分为两类[4]，一类是有线通信接口，如USB、*RJ45*、*RS*232和PCI Express等；另一类是无线通信接口，如Wi-Fi、GPRS、蓝牙、红外线等。这些接口虽然使打印机的功能得以扩展，但也增加了非授权用户窃取打印数据的途径。

第二，网络接入泄密。当前，打印机正在向着综合信息管理与输出终端方向发展，大都集成了丰富的网络功能。这些功能在提高工作效率，提升团队协作能力的同时，也成为信息泄露的一个主要渠道[7]。当打印机被接入外部网络（如Internet）时，打印机将不可避免地与公共网络产生数据交换；此外，一些开放端口甚至能够被黑客利用[7]，导致打印机被非法接管。

第三，数据传输泄密。计算机在将打印作业下发到打印机的过程中，需要通过数据传输介质与打印机进行数据交互。这一过程中，如果打印数据在传输前未进行加密，在传输过程中一旦被入侵者非法劫持，入侵者能够很容易地通过协议分析工具得到真实的打印数据。

2.2 硒鼓泄密风险

硒鼓是打印机的核心部件之一，用于接收激光扫描模组发射的激光图像数据，通过静电高压的配合将图像转移到纸张上实现打印输出。它主要由感光鼓、带电辊和碳粉盒组成[8]。硒鼓主要有以下泄密风险点。

第一，感光鼓表面静电残留泄密。打印机每打印完一份文件，其感光鼓表面会存在一定的静电残留，这些残留电荷的分布状态与打印图像是一一对应的。因此，通过对静电分布状态进行识别，能够对打印内容进行复现，从而导致信息泄露。

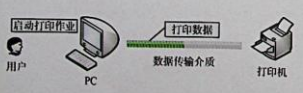

图1 打印数据传输过程

第二，在硒鼓内植入芯片。为了统计打印页数和碳粉使用情况，打印机厂商通常会在硒鼓中内置低压电路和芯片模组，这就为窃密者提供了在硒鼓上安装存储芯片或无线通信模块的条件。通过这些装置，重要信息可能就被悄无声息地非法存储和发送了。

第三，有机感光导体（Organic Photo-Conductor，OPC）潜像残留泄密。在打印作业完成后，硒鼓的OPC部件可能仍然保留着已打印图像的潜像，这些潜像信息如果得不到及时清理，可以被二次打印。

2.3 打印机存储器泄密风险

为了适应日益繁重的打印任务，提升打印机性能，打印机厂商会在打印机中配备存储器，如内存、存储卡和硬盘等[9]。这些存储器主要有以下风险点。

第一，内存数据泄密。通常，打印机在接收到计算机的打印任务后，首先会将待打印数据暂时存储在内存中。当打印作业完成后，若打印机内存中的打印数据未被及时清理，很容易被非法读取和复现。

第二，永久性存储器泄密。由于内存价格高昂，一些廉价打印机配备的内存相对较小。为克服内存不足的问题，厂商会在打印机中安装存储卡或硬盘等永久性存储器。打印机工作时，首先将待打印数据存入永久性存储器，打印时再读入内存。由于永久性存储器断电后数据不清零，且方便拆卸和携带，打印机中若配备此类部件，很容易导致打印数据被非法窃取。

2.4 打印机软硬件泄密风险

打印机整体上可划分为软件和硬件两个部

分。硬件包括机械部件、电路和耗材等，软件包括SOC固件、驱动程序和审计管理系统等。打印机软件和硬件主要有以下风险点。

第一，软硬件安全性不可控。当前，国内打印机市场仍然被国外品牌（如惠普、三星等）主导，国产打印机品牌虽然有所发展，但核心部件仍然依靠进口，缺乏自主知识产权。由于打印机结构复杂，设计精密，很容易在其内部安装非法部件或植入恶意代码，且此类隐患难以被察觉。因此，国外打印机软件和硬件的安全性和可靠性不可控。

第二，固件泄密。为了方便打印机维护，改善打印机功能，厂商一般会为打印机提供固件升级功能，而固件升级是黑客植入恶意代码的主要途径。当含有恶意代码的固件被安装到打印机后，这些非法程序将对打印内容进行监视和记录，并通过邮件等方式发送打印内容，甚至篡改和破坏打印数据。其泄密过程如图2所示。

第三，电磁辐射泄密。打印机在工作过程中将不可避免地产生电磁辐射，这种电磁辐射可能携带打印机处理的打印信息[10]。入侵者可通过对捕获的电磁辐射进行分析，将真实打印信息提取和呈现，从而导致信息泄露。

2.5 打印管控泄密风险

通常情况下，当用户通过内部网络将打印文件从计算机下发到打印机后，打印机会立即执行打印操作，如果用户和打印机之间存在一定距离而无法及时取走已打印文件时，打印文件存在被窃取的可能[11]。此外，涉密场所的打印作业管理通常依赖于保密管理制度的强制实施和人工监管，这虽然在一定程度上维护了涉密信息的安全，但仍然存在着诸多不便和风险隐患。分散的打印输出方式不利于安全保密管理，打印设备使用权限难以有效控制，打印审批效率低下。这些问题很容易导致非授权用户非法窃取重要信息。

3 打印机安全风险防范措施

通过上述分析可以看出，打印机在打印作业过程中存在诸多安全风险。针对以上问题，本文提出以下对策。

（1）关于通信接口泄密

通信接口是打印机与外界进行数据交互的主要渠道，防止通信接口泄密应从以下两方面着手：一是打印机厂商应避免配置多余外部通信接口，只保留以太网接口和USB接口等必要通信接口，并严格控制每种接口的数量；二是管理员应能够对通信接口的开启和关闭进行管控，并且在默认情况下通信接口应处于关闭状态。

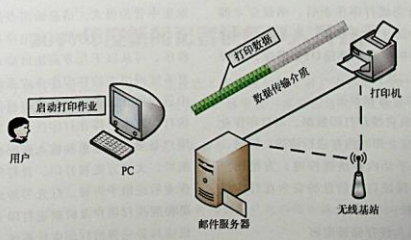

图2 固件泄密过程

（2）关于网络接入泄密

防止打印机产生网络接入泄密，重点是保证重要信息系统网络中的打印机与外网物理隔离，可以从以下两方面着手：一是打印机应被限定在固定场所内使用，并且只能通过内部网络进行打印作业；二是打印机一旦与外网连接，应给予声音、灯光等形式的警告提示，或以内网邮件形式通知管理员，并能够立即切断与外网的连接。

（3）关于数据传输泄密

防止数据传输泄密需要从以下3个方面着手：一是用户向打印机下发的打印数据需经过加密处理后再进行传输，从源头上保证打印数据的安全；二是厂商应为打印机部署私有协议，保证打印数据通过区别于通用协议的本地私有协议进行传输；三是传输介质宜选用经过严密防护的数据电缆或光纤，防止打印数据被物理劫持。

（4）关于硒鼓泄密风险

硒鼓是打印机的核心部件之一，也是打印机泄密的主要途径之一。防止硒鼓泄密，一是保证硒鼓中不配备任何形式的电路板和芯片，防止打印数据被非法窃取；二是硒鼓应具备静电清除能力，当完成打印作业后，硒鼓应立即释放残余电荷，防止静电残留；三是每打印完一份文件，打印机应自动擦除OPC潜像，确保已打印资料不被二次打印。

（5）关于内存数据泄密

打印机内存负责缓存打印数据，当打印作业完成后，打印机应立即对内存进行清除；同时，打印机还应具备手动内存清除按键，方便用户手动清理内存，保证打印信息的安全在打印机中的生存周期可控。

（6）关于永久性存储器泄密

永久性存储器能够轻易地记录打印信息，且不易丢失，是打印数据泄露的重要途径之一。因此，厂商不应为打印机配备硬盘、存储卡或存储芯片等形式的永久性存储器，杜绝打印数据、用户信息和主机信息被非法存储。

（7）关于软硬件安全性不可控

打印机主要核心部件，如硒鼓、中控等应具备自主知识产权，并为国内正规厂商自主研发、生产和制造，保证打印机硬件和耗材的安全可控。此外，打印机管理系统和驱动程序应由打印机厂商自主开发，保证打印机软件的安全可控。

（8）关于固件泄密

固件是打印机的核心软件，保证打印机固件安全，可以从以下两方面着手：一是要求打印机具备对非法固件的主动识别能力，如可在固件中加入唯一性可信凭据，只有通过了验证的固件才被允许安装；二是当打印机检测到非法固件时，应拒绝安装，并立即删除非法固件，同时向管理员发出警告。

（9）关于电磁辐射泄密

打印机工作时产生的电磁辐射可能携带打印信息，电磁辐射强度不达标，将使辐射电磁信息被非法获取和复现。因此，打印机出厂时应通过严格的质量检验，保证其电磁屏蔽性能达到国家相关标准要求。

（10）关于打印管控风险

在重要信息系统网络中，信息的输出应采取集中管控模式，信息输出点配置规则应遵循最小化原则。同时信息输出应具备严格的审计程序，可从以下几方面加以应对：一是重要信息系统网络中的打印作业应采取集中打印和集中管理模式，保证信息输出可控；二是采用可信打印技术。即在打印任务下发至打印机后，用户必须在打印机端输入密码、指纹等可信凭据后，文档方能被打印，且打印机在完成打印作业后应给予声音、灯光等形式的反馈信息，以提醒授权用户及时取走打印文件；三是打印机应具备完善的打印审计系统，且管理方便，界面友好，同时审计系统应具备明确的管理员权限划分，且不同管理员之间应相互独立，相

互制约，分工明确；四是审计系统应具备全面、丰富的安全策略控制项，能够对用户的打印权限进行细粒度的审批和授权，并能够清晰、准确地记录用户和管理员的打印和操作日志，便于事后溯源。

4 结语

重要信息系统网络的安全保障是一项复杂的工程，任何地方出现纰漏都有可能造成严重的后果。打印机作为重要信息系统网络中必不可少的环节之一，对重要信息系统网络的安全威胁不容忽视。本文分析和研究了重要信息系统网络中打印机所面临的各种泄密风险点，并从技术措施和管理手段两方面提出了相应的防范措施。希望本文研究的内容能够为国产打印机安全性的改进和重要信息系统网络中打印安全风险的防范提供借鉴。

参考文献：

[1] 朱耀庭.个人打印机综述 [J].个人电脑,1997(03):60~76+81~95.

[2] 本刊.打印安全 [J].办公自动化,2011(23):39.

[3] Everett C.Printers: the Nneglected Threat[J].Network Security,2011(09):8~11.

[4] 庄海燕,王刚.网络打印机安全分析与防范[J].网络安全技术与应用,2007(05):50~51.

[5] 孙梦云.打印机技术的历史演变与当代发展[D]:上海:华东师范大学,2014.

[6] 杜冲.分布式安全打印关键技术研究[D].西安:西安电子科技大学,2013.

[7] Gengler B. Network Printers Pose Security Risk,CERT[J].Network Security,2001(12):5.

[8] 翁芸娴. 硒鼓的结构设计及打印品质研究[D].苏州:苏州大学,2013.

[9] Canon Warns of Digital Printer Security Issue[J].Infosecurity,2010,7(04):7.

[10] ISO/IEC 11160-2:2013. Information Technology --Office Equipment--Minimum Information to be Included in Specification Sheets--Printers --Part 2: Class 3 and Class 4 printers [M]. Switzerland ISO/IEC.2013:17.

[11] 王飞.安全打印与审批系统的设计与实现[D].西安:西安电子科技大学,2014.