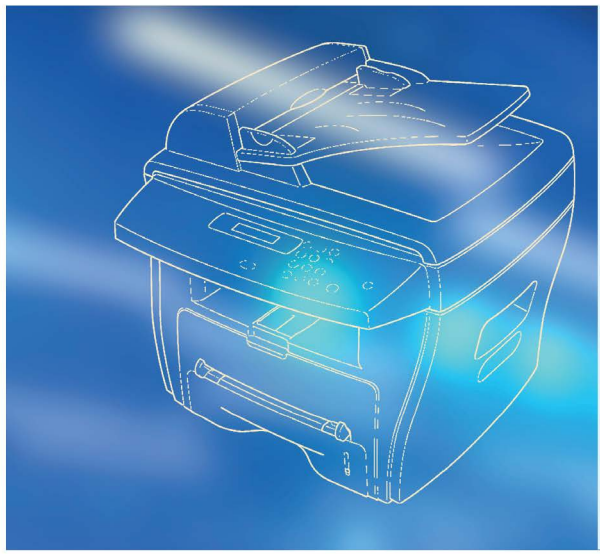
别让打印机成为校园网络安全盲区

文 / 郑海山 林霞 洪江民 萧德洪

高校打印机面临的安全问题及解决思路



网络打印机可能支持打印、扫描、传真、复印等功能，支持有线网络、无线网络、USB 直连、网络共享、Wi-Fi Direct，云打印等模式。网络打印机一般使用精简 Linux 或者实时操作系统，实际上本身已经是一台小型的服务器，应当做好相应的安全保护。

打印机作为工作中最常见的办公设备，因为责任人不清、责任人安全意识薄弱导致打印机成为了严重的信息泄露源和安全盲区。打印机相比数据中心服务器，通常缺乏必要的关注和安全防护。有报告指出，每天大约有 8 万台打印机对互联网暴露[1]。这些暴露的打印机会导致包括但不止于拒绝服务攻击、特权升级或绕过、操作或读取打印内容、信息泄露、远程代码执行、漏洞利用等问题[2]。高校内各个部门或者实验室均会配备至少一台网络打印机，如果打印机由于配置错误或者漏洞导致被攻陷，会对使用打印机和内网的用户造成严重威胁[3]。李莉等[4][5]分析了网络打印机存在的风险并提出了防护建议，史岗[6]和郭磊[7]从保密层面对打印机安全性进行了分析并给出了防范措施。

网络打印机智能化程度提高，复杂的功能带来了对打印机维护人员较高的技术能力要求。网络打印机品牌众多，管理界面复杂，可配置项多，为了方便用户开箱即用，往往所有协议、服务和功能全部开启，没有任何安全配置。网络打印机可能支持打印、扫描、传真、复印等功能，支持有线网络、无线网络、USB 直连、网络共享、Wi-Fi Direct，云打印等模式。网络打印机一般使用精简 Linux 或者实时操作系统，实际上本身已经是一台小型的服务器，应当做好相应的安全保护。

高校校园网有边界防火墙，可以阻挡打印机部分端口对外开放，有些学校对用户网段和服务器网段分开，用户网络限制不能对外提供服务，这些安全措施从一定程度上缓解了网络打印机造成的风险，然而在校园网内部，如果未做好安全域隔离，网络打印机的安全风险在校园网内部还是存在。对于网络打印机的安全性整改，解决思路为从管理和技术两个层面进行。管理上通过内部公文系统下发打印机安全配置等相关要求，技术上通过全网扫描打印机，对未加固的打印机进行多轮通知整改，达到最终所有打印机均做好较为安全的设置。

打印机安全整改流程

从管理层面入手，通过出台物联网设备安全管理方法，网络打印机专项安全防护细则等规章制度，首先从主体责任和安全意识入手，引起各部门和普通用户对打印机安全性的重视。通过管理层面，可以解决一部分问题，然而有些用户思想上重视了，但是由于技术能力和其他客观因素，导致整改不到位，所以需要配合技术手段进行常态化检查。

由于网络打印机如果未做好安全配置，在校园网内是可以随意访问的。我们从攻击者视角，使用简单的 Python 脚本，对暴露在校园网内的多轮通知未整改的打印机进行发现和检查，并且采用打印通知信息到用户打印机的方法通知用户。

1. 发现：

我们使用 nmap 扫描校园网内所有网段网络打印机常用的

515、631、9100端口，如果这些端口开放，则记录到可能的打印机列表文本文件内。

2. 取证：

由于发现机制存在一定的误报可能，所以我们对可能的打印机IP进行指纹识别，通过人工筛选等方法尽量做到误报率最小。我们对可能的打印机列表文本文件，每一个IP地址，均使用ipptool命令获取打印机的元数据，主要包括打印机制造商、型号、打印机名称、打印机UUID、打印机WiFi连接信息、固件版本和开机时间，将可以获得的元数据存入打印机元数据列表文件内。接着对可能的打印机列表文件，每一个IP地址，使用Python模块pyppeteer获取HTTP端口上的网页标题和截图，并保存成图片。

3. 分析：

我们接着对端口开放情况、元数据、网页标题、截图进行排查，识别出校内打印机类型和分布情况，剔除误报的IP。并直接连接到打印机获取部分配置信息，形成校园网内网络打印机安全性报告。

4. 通知：

我们根据IP段归属对IP段管理员进行通知，对于多次通知仍未处理的打印机，我们使用Python脚本将一张拟好的通知A4纸内容打印到用户打印机上。具体为使用lpadmin命令行根据打印机IP地址添加打印机，使用lpr命令行打印出通知文本，打印完毕删除打印机完成通知。

5. 整改：

在通知文本内，我们提供了群号，要求所有看到通知的用户联系打印机责任人加群，在群内下发整改具体方法和解答用户的疑问，并且最终整理入常见问答内。

因为打印机资产随着时间会有所变化，所以我们通过定期多轮实施以上流程进行整改。对于打印机的发现，如果有全网认证系统或者有收集所有设备IP地址对应的MAC的数据库，也可直接从MAC地址前缀识别出打印机。对于通知，如果已经有建立了比较完善准确的IP对应用户数据库，也可直接通过邮件或者其他渠道通知，实践证明，直接打印通知到打印机对用户的震慑比其他通知手段效果更为明显。

打印机安全配置和使用最佳实践

在网络打印机安全专项整改中，我们分析了各个不同类型的打印机的功能，并给出了几十项安全检查点要求打印机管理员逐项检查。检查点按角色归纳如下：

1. 管理部门

要求各部门应明确主体责任，确定专门的打印机管理员；对打印机建立台账跟踪打印机全生命周期管理和定期安全检查记录；定期对打印机管理员和用户进行安全培训；定期对内网暴露的打印机进行通知整改；对关键部门进行保护，减少用户不规范使用带来的安全问题。

2. 打印机管理员

应当采购具有安全能力的较新的打印机；对存量打印机进行复位并重新做好安全配置；修改默认密码为强密码，遵循最小权限原则关闭所有不必要的服务和协议；限制IP地址访问控制列表；应定期清空格式化打印机敏感信息；定期检查打印机是否会对外发送数据；配置本地发送邮件的SMTP服务器；定期从官方源更新打印机固件；打印机场内场外维修应当做好防止信息泄露措施；在报废之前应当复位，销毁内部存储芯片，拔除硬盘和存储卡。

3. 普通用户

应当尽量使用点对点方式（USB、FTP、网上邻居）接收扫描敏感内容，如配置了FTP和网上邻居等服务应做好安全防护，密码应当设置强密码，并且设置防火墙只允许打印机访问；扫描完的文件应当移出FTP或网上邻居目录；敏感文件应当改名再打印；应当尽量只采用操作系统自带的打印能力，如果安装了打印机厂商提供的打印软件，应当定期更新打印软件。

通过管理手段和技术手段相结合，通过常态化检查，可大大提高校园网内打印机的安全性。本文的打印机技术发现手段只能识别联网打印机，如果是直接连接计算机的打印机，只能从管理层面进行整治。本专项治理思路和流程未来可以扩展到其他物联网设备诸如摄像头、门禁、考勤机、大屏幕、内网交换机、路由器、中控系统、贵重仪器设备、工控设备、各类联网传感器等。

CEN（责编：郑艺龙）

（作者单位为厦门大学信息与网络中心）

参考文献

[1] SHADOWSERVER. Open IPP Report - Exposed Printer Devices on the Internet[EB/OL][2020-06-10]. https://www.shadowserver.org/news/open-ipp-report-exposed-printer-devices-on-the-internet/.

[2] JENS M. Hacking Printers[EB/OL][2020-07-06]. http://hacking-printers.net/wiki/index.php/Main_Page.

[3] KRITKORN K, CATTALYYA N, KORRAWAT P, et al. Hacking Printers: MIT's Printers Security Analysis[EB/OL]. (2018-05-16)[2020-07-06]. https://courses.csail.mit.edu/6.857/2018/project/kritkorn-cattalyy-korrawat-suchanv-Printer.pdf.

[4] 李莉，陈诗洋，杨子羿，等. 网络打印机安全研究与防护建议[J]. 电子产品世界，2019，26（3）：58-61.

[5] 天地和兴工业网络安全研究院. 打印机主要网络安全问题及改进建议概述[EB/OL][2020-07-06]. https://www.secrss.com/articles/23521.

[6] 史岗，李姗. 打印机安全风险与防范解析[J]. 保密科学技术，2017（1）：26-29.

[7] 郭磊，刘博，崔中杰. 打印机信息安全风险与防范措施研究[J]. 保密科学技术，2018（01）：43-47.