Security and USB Ports on Lexmark Devices

Version 2.1

October 2010

LEXMARK

Contents

Applicability

This white paper applies to the following Lexmark products:

- Lexmark E460 Series Laser Printers
- Lexmark X460 Series Multifunction Printers
- Lexmark T650 Series Laser Printers
- Lexmark X650 Series Multifunction Printers
- Lexmark W850 Series Laser Printers
- Lexmark X860 Series Multifunction Printers
- Lexmark C730 Series Color Laser Printers
- Lexmark X730 Series Color Multifunction Printers
- Lexmark C792 Family Color Laser Printers
- Lexmark X792 Family Color Multifunction Printers
- Lexmark C925de Color Laser Printer
- Lexmark X925de Color Multifunction Printer

This white paper does not constitute a specification or warranty. All rights and remedies concerning products are set forth in each product's Statement of Limited Warranty.

Abstract

USB connectivity is now prolific among computers and peripherals.

Lexmark's printers include support for attaching devices via USB and have extensive security. measures related to the use of such devices.

Virtually every personal computer sold today contains Universal Serial Bus, or USB, ports by which a wide array of devices can be attached. As with most technologies, the nature of USB support involves a measure of security exposure, since most anything that can be used can also be abused — theoretically if not practically.

Many Lexmark laser printers and multifunction printers (MFP) include support for USB devices, and it is appropriate to consider the potential security ramifications of that support. This white paper describes the security considerations related to USB ports on Lexmark devices, and explains the protections that have been put in place to address those security concerns.

Executive Overview

USB ports on Lexmark printers allow "thumb drives" to be attached.

Image files can be printed from the thumb drives.

The thumb drive may not be used to perform other operations on the device, such as changing or retrieving configuration information.

USB ports on personal computers provide a means to connect devices of various types and perform a variety of interactions. However, for security reasons the USB ports on Lexmark devices are far more limited in their capabilities.

The USB host ports on Lexmark's devices provide the following:

- When a USB mass storage device (such as a thumb drive) is inserted, the printer finds and displays by name the image files and/or flash files that are stored on the device.
- The user can select jobs to print from the displayed jobs. If a flash file is selected, the printer firmware will be updated as long as firmware updates are allowed in the security settings.
- Additionally, a user can scan data directly to the USB thumbdrive if it is available in a supported scan format.

The USB host ports on Lexmark devices disallow the following operations:

- The connection and use of any form of USB device except a mass storage device, card reader or human interface device (HID), such as a keyboard.
- The submission or processing of PCL, PostScript, or other printer datastream files.
- The submission of any other sort of data (executable code, configuration files, etc.).
- Recording any sort of data from the printer to the USB-attached device other than direct scan to USB thumbdrive jobs.
- Executing code from the USB-attached device.
- Booting the printer from the USB-attached device.

- Transferring data between the USB-attached device and the network to which the printer is attached (note: except in cases where the device is configured to use the USB port for authentication using a smartcard).

  Disabling the USB port is an option at manufacturing or by the device administrator during setup.

Two Types of USB Ports

There are two types of USB ports to consider, related to Lexmark laser printers and MFPs:

1. ***USB Device Ports***. This type of port is generally not considered a security concern.

   USB device ports have been a standard fixture on printers and MFPs of all sorts for several years. These ports are typically on the back of the printer or MFP, and allow the device to receive print jobs from the computer to which the device is attached. The primary purpose of the USB device port on the back of the printer or MFP is for the device to receive data.

2. ***USB Host Ports***. This is the type of port that is generally interesting in a security discussion.

   Lexmark laser printer and MFP families include a USB host port on the front of the devices. Although host ports are how many types of devices are connected to computers, Lexmark's printers carefully restrict the operations that can take place over these ports in order to avoid security exposures to the products or to the customers' environment. Additionally, device administrators have the ability to disable or restrict access to USB host ports through the use of authentication and authorization function access controls, which can be tailored to meet the requirements outlined by a customers' network security policy.

USB Support on Lexmark Devices

USB support on printers and MFPs is not like USB support on personal computers, in general. Personal computers typically support a wide array of devices through USB, such as keyboards, mice, monitors, hard drives, speakers, network cards, digital cameras, and others. The flexibility offered by USB host support on personal computers is not needed—or desirable—on printers.

Image files can be read from USB devices, but the printer protects itself from all other interactions with the device.

The purpose of the USB host port on Lexmark devices is to allow convenient printing and scanning of image files for end users and fast, easy serviceability via firmware updates for technicians.

The supported image file formats are .pdf, .xps, .gif, .jpeg, .jpg, .bmp, .png, .tiff, .tif, .pcx, and .dcx. Please note that the device's firmware and the USB host port implementation are carefully designed to restrict the use of the port for any other purpose.

A number of factors in the design provide for that protection, including:

Support Limited to Mass Storage Devices

Only USB hard drives are supported—there's no support for USB network adapters or other forms of USB compatible devices.

When a USB device is connected to a USB host port (like the one on the front of Lexmark laser printers and MFPs), a process known as enumeration occurs. The device indicates its device class to the host so the host knows how to communicate with it.

Lexmark devices only support devices that enumerate with a Mass Storage device class. This means if a device such as a USB network card is inserted, the printer will refuse to establish a connection to it. USB "thumb drives" are a typical example of the sort of device one would expect to use with a printer or MFP. These devices are prolific today, and are generally supported by printers and MFPs.

Devices that are SCSI compliant, use the FAT32 file system, and do not include an embedded hub are likely to be recognized and compatible with a Lexmark device. If the USB device does not meet the requirement outlined above, then the printer or MFP will reject the device as unsupported.

Support Limited to Printing Image Files, Direct Thumb Drive Scanning and Updating Firmware via Flash File

Only image files can be printed or scanned to a USB device. Misnaming a file or its extension doesn't fool the printer or MFP into accepting the file as a supported file format.

When a USB thumb drive is inserted into the device's USB host port, the printer or MFP examines the file system of the inserted device and displays a list of the image files (.pdf, .xps, .gif, .jpeg, .jpg, .bmp, .png, .tiff, .tif, .pcx, and .dcx) and firmware files (.fls) on the device. No other type of file is displayed, or supported. Files that contain PostScript or PCL datastreams are not supported.

When the user elects to print a file, the contents of the file are read from the USB-attached device and transferred to the appropriate image interpreter. This component of the device's firmware inspects the format of the file, and discards files that are not of the indicated format. Also, firmware files are only accepted on the device if they have been signed by Lexmark, ensuring that tampered firmware can never be installed on your device. This eliminates any opportunity to submit a file by mislabeling it; in other words, a person cannot put executable code onto the printer by storing it in a file called "Harmless Job.pdf".

Note that the image files are treated internally just as if they were submitted to the device via any of the other device ports (parallel, network, etc). This means that the USB host port doesn't provide any avenues for submitting data that didn't already exist. In many regards, the USB host port is less forgiving since it is up to the printer to display and allow the submission of data through the USB connection. Unlike the other connections, the printer has some say in what is sent to it via USB.

There is no support for submitting executable code, code updates, configuration changes, or anything other than .pdf, .xps, .gif, .jpeg, .jpg, .bmp, .png, .tiff, .tif, .pcx, and .dcx files to the printer via the USB host port.

No Support for Booting from a USB-Attached Device

On many personal computer systems, the USB host port is included in the list of bootable partitions—meaning, one can potentially boot such computers from the thumb drive. This is not the case on Lexmark printers and MFPs. The USB ports are not included in the boot sequence in any way.

No Support for Network Interaction with USB-Attached Device

The USB-attached device cannot exchange data with the network to which the device is attached in any way. There is no facility for passing data from the USB-attached device to the network or from the network to the USB-attached device.

The only exception would be cases where the printer or MFP provided authentication capabilities through a human interface device (HID) such as a card reader for card-based authentication. In this instance, an embedded application would be installed through the Lexmark Embedded Solutions Framework on the printer or MFP. This application creates the ability for the device to interface solely with a directory server to validate the identity of a user, pull information associated with the authenticated user (for example, e-mail address and home directory information) and identify privileges associated with that user.

No Support for Adding Additional Drivers or Functionality

The functions that are allowed or disallowed with USB-attached devices are controlled by the printer or MFP's firmware, which is not customizable or extensible by the end user. The device's firmware disallows the addition of arbitrary executable code of any sort.

Firmware updates, which are supported via the USB device port on the back of the printer or MFP and via the network interface, must include multiple digital signatures. This ensures that the printer or MFP will only accept code that is produced and provided by Lexmark International Inc. Even then, the code cannot be transferred via the USB host port—only by the other conventional avenues.

There is no support for adding additional USB drivers to the printer to alter the function of the device.

USB Host Port Can Be Disabled

There are some environments where controlling the submission of print jobs (including image files) is important and all uncontrolled avenues by which jobs could be submitted are undesirable.

For example, in a college library there may be a system by which users can submit print jobs over the network, and be charged for the pages they print. In such a case, it would be unacceptable to allow users to walk up and submit jobs to the printer from a USB thumb drive.

The USB port can be disabled at the point of manufacturing or by the customer through the device's EWS.

Customers have two options for disabling the function of the USB host port entirely. The first is for Lexmark to disable the port during the manufacturing process. In that case the port is permanently disabled and may not be reactivated by the device administrator or end user under any circumstances.

On a printer or MFP that has not been altered during manufacturing, the device administrator can disable the port through a menu on the device's embedded web server (EWS). In this case, the port can be enabled again at a later time should the need arise. Note that the function of disabling or enabling the port can be restricted so that end users cannot re-enable the port.

Summary

USB ports on Lexmark devices do not expose the device to abuse.

Unlike USB host ports on personal computers, the USB host ports on Lexmark devices are limited to a well-defined set of functions. That functionality involves the printing and scanning of image files and facilitating firmware updates for easy serviceability.

The nature of USB is such that the host—in this case the printer or MFP—controls the interaction between the USB client device and the host. Lexmark printers and MFPs are designed to allow only a carefully controlled set of functions, which do not expose the printer to abuse or manipulation by the client device.