technical **white paper**

> Security Features of Lexmark Laser Printers: Overview

Sean Gibbons
Technical Security Consultant
March 2007

Contents

Executive Summary

Printers are complex network devices that require careful consideration regarding security. Lexmark's printing and networking products include a wide array of security related features. This document discusses those features and provides an overview of their benefits and their implementation.

Any device that is placed on a network must be evaluated with respect to security. How does the device protect itself from unauthorized access? Does the device expose the network to any form of vulnerability? What sort of information does the device process, and what are the security considerations related to that data? These and many other questions are appropriate to ask of any networked device, including networked printers.

Networked printers operate independently on the network and can be focal points for sensitive information. Securing them is sometimes comparable to securing other conventional networked devices such as computers: the need for controlled network access and the need for secure remote management are largely the same for printers and workstations. In other areas, the security considerations around printers are substantially different: they generally don't run conventional operating systems, they don't have network file shares that need to be secured, they probably don't need or support antivirus software, etc.

This document will define the major areas of security concerns related to printers, and provide an overview of the security features of Lexmark's printers that allow the devices to be deployed, managed and used in a secure manner.

Applicability

This white paper applies to the following Lexmark products:

- Lexmark C522 laser printer
- Lexmark C524 laser printer
- Lexmark T640 laser printer
- Lexmark T642 laser printer
- Lexmark T644 laser printer
- Lexmark C780n laser printer
- Lexmark C782n laser printer
- Lexmark W840 laser printer
- Lexmark C920 laser printer
- Lexmark C935n laser 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.

Secure Device Management

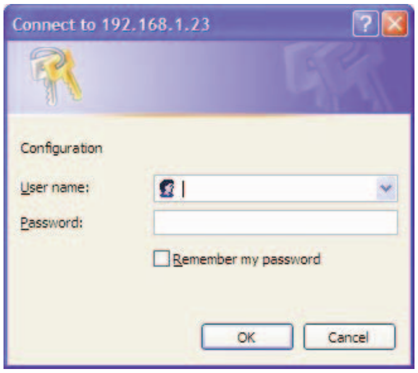
To practically manage a fleet of networked printers, remote management is a must. But the remote management must be secure. The device must allow authorized people to configure it while rejecting those that are unauthorized. The process of managing the device must also be secured so that the network traffic associated with the remote management can't be sniffed or stolen, and abused.

Lexmark's printers include a variety of features to make remote device management easier, and more secure.

Network Password

Overview

The network password keeps unauthorized people from using a browser or other network tool to configure the printer. Users can point their browser to the printer on the network and see the basic status of the device, but any attempt to configure the printer results in a challenge for the password. If the user can't provide the password, then configuration of the printer is not allowed.



When an attempt is made to configure the printer via the web browser, the printer's password must be provided.

Benefits

This basic "building block" of security allows the right people—and only the right people—to configure the device.

Details

The password can be up to 128 characters in length, and supports alphabetic, numeric and other characters to allow for substantial complexity. The password is not associated with a user name, and there's no support for creating additional administrative accounts—there's just one administrative account, and this password controls access to it. (The ability to create additional accounts can lead to more vulnerabilities by allowing undetected and potentially long-lasting accounts to be created.)

Once the password is in place, it must be provided in order to configure the printer via the web interface, through MarkVision Professional or through telnet[1].

Operator Panel PIN

Overview

To protect the printer from unauthorized configuration via the printer's operator panel, the printer can be configured with a 4-digit PIN code with a range of 10,000 values. When an attempt is made to configure the printer via the operator panel, the printer prompts the user for the PIN. Unless the proper PIN is entered, the printer's settings cannot be changed.

Benefits

Like the device password, the PIN keeps unauthorized users—even those that have physical access to the printer—from configuring the device. This can protect against malicious or accidental configuration changes.

Details

The PIN is 4 digits of a value 0-9, and is set up through the printer's web page. It can be applied to all of the settings accessible through the operator panel, or it can be selectively applied to the sections of the printer's menus that deal with paper settings, general device settings, reports, and network/port settings.

HTTPS

Overview

The most common means to remotely configure a printer is through the printer's web pages. Point your browser to the printer's IP address or DNS name, and if you can provide the printer's password (as described above in Network Password) you can configure the device's settings.

However, browsers and the HTTP traffic associated with them are not inherently secure: someone could sniff the network traffic used in the web session and determine the device's password. To address this concern, Lexmark's printers support HTTPS.

Benefits

The benefits of using HTTPS for web sessions include:

- The process of establishing the connection is extremely easy for the end user: the browser just needs to be pointed to https:// instead of http://. The rest is automatically taken care of by the printer and the browser.
- All data exchanged through the browser is encrypted—this includes the printer's password and any other settings that are specified or viewed.
- HTTPS and SSL are extremely prolific standards, supported by all of the most commonly used web browsers.

[1] Note that the amount of configuration available through the telnet interface is limited, and for further security that interface can and should be disabled. The process of disabling unused or unwanted interfaces is covered in the Device Hardening section of this document.

- The printer's certificate that allows the SSL session to be established can be signed by a certificate authority, allowing it to integrate into preexisting CA or PKI environments.

With HTTPS, web sessions can be conveniently and effectively secured.

Details

The printer includes an embedded web server, and when a browser is pointed to the printer's address with the https:// prefix the printer and the client system negotiate an SSL connection. This involves the printer passing its x.509 certificate to the client system, to establish its (the printer's) identity. Since the printer's certificate is, by default, self-signed, the client will typically present a warning to the user (whether and how this happens depends on the settings of the web browser). The client system can choose to trust the self-signed certificate, and thereafter receive no further warnings.

Alternatively, the printer's certificate can be signed by a certificate authority (or CA). This can be an external CA, or—more likely and more practically—a CA that's internal to the customer's environment. The printer's web interface includes a Certificate Management page that facilitates this process.

Replacing the self-signed certificate with a CA-signed certificate avoids the warnings associated with HTTPS sessions.

The HTTPS session is built on an SSL connection, in which all exchanged data is encrypted. This protects the contents of the session from eavesdropping, and allows for secure remote management of the printer.

SNMPv3

Overview

SNMP (Simple Network Management Protocol) provides another means to remotely configure printers. It can be used to view and alter printer settings, so it involves the basic security questions of how to control its use and how to protect the associated network traffic when it is used.

Lexmark printers support the latest version of SNMP, version 3. This standard protocol includes support for authentication, and for data encryption. Lexmark printers also support SNMPv1 and v2 for backward compatibility.

Benefits

Support for SNMPv3 allows Lexmark printers to be managed securely by standard SNMP console applications. There are two important elements to the security provided by SNMPv3:

- Authentication allows authorized systems to see and manage the printer via SNMPv3, while shutting out unauthorized systems.

- Encryption of the SNMPv3 packets protects the information from being sniffed from the network. Or, more accurately, the sniffed data is useless because it's encrypted.

Details

The authentication features of SNMPv3 allow the printer to refute SNMPv3 traffic unless the requests are preceded by an authentication (via MD5 or SHA1). The printer supports two SNMPv3 accounts: authenticating against one yields the ability to read the printer's settings but not write them, authenticating against the other provides the right to read and write the printer's settings.

Support for data privacy in SNMPv3 means that the printer and SNMP client can use an encryption algorithm (DES, or AES with 128, 192, or 256 bit keys) to encrypt the SNMPv3 traffic.

As with other mechanisms for managing the printer, SNMP can be disabled—if it's not used in a particular environment, it can be and should be turned off entirely.

IP Security (IPSec)

Overview

IPSec (IP Security) is supported on Lexmark's printers. This is an extremely important mechanism, since it allows the printer to establish a secure connection to other network nodes such as print servers and management workstations.

IPSec is available on conventional operating systems (Windows, Linux, etc.), and by applying IPSec between the printer and a workstation or server the traffic between these systems can be secured with strong encryption.

Benefits

IPSec can provide many benefits, including:

- When IPSec is used between the printer and the print servers that route print jobs to it, the content of the print jobs is protected from network eavesdropping. By extending the IPSec connection between the print servers and the client systems, the entire print path can be secured.
- When IPSec is used between the printer and the workstations of administrators, remote configuration (by a web session, telnet, SNMP, or any other IP-based means) can be secured. Since mechanisms like HTTPS and SNMPv3 can provide their own security, as described above, IPSec can be used as part of a "Security in Depth" architecture to provide multiple levels of protection. Or, IPSec can be relied upon to provide the security, simplifying the other mechanisms.
- When IPSec is used between the printer and a server running Lexmark's management application, MarkVision Professional (MVP), all communications between the MVP server and the printer is protected.

In short, IPSec can be used to protect virtually any form of IP-based network traffic between the printer and a set of hosts, no matter what operation is performed by that traffic.

Details

Lexmark printers support IPSec with preshared keys and with certificates.

In preshared key mode, the printer can be configured to establish a secure IPSec connection to up to five other systems. The printer and these systems are configured with a pass-phrase, which is used to authenticate the systems and to encrypt the data subsequently.

In certificate mode, the printer can be configured to establish a secure IPSec connection to up to five other systems or subnets. This allows the printer to exchange data securely with a large number of systems, and the use of certificates allows the process to be integrated with a PKI or CA infrastructure. This provides a more robust and scalable solution, without the burden of configuring or managing keys or passphrases.

The printer can store and apply two certificates for use with IPSec. The printer includes a self-signed certificate that can be replaced with a certificate signed by a CA. This certificate can be generated from scratch, or it can be generated with the base64 encoded PKCS file that's embedded in the printer and available through its web interface. This allows the printer's identity to be validated by other systems in the CA environment. In addition, the printer can store the CA's certificate as a trusted root CA certificate, allowing it to validate the identity of other systems in the CA environment.

IPSec can be used in preshared key mode and certificates mode, simultaneously.

802.1x Support

Overview

In almost all network environments, users are required to log on to the network before they can do things like send or receive email, browse the web, etc. This can be taken to another level, where devices such as laptops—or printers—can be required to authenticate before they are allowed on the network. The protocol for performing this authentication is 802.1x. Lexmark's printers support the 802.1x for device authentication.

Benefits

802.1x provides the following benefits:

- It allows the printer to authenticate itself to the network for increased security.
- With support for a wide array of authentication methods, the 802.1x authentication method will be compatible with almost any 802.1x authentication environment.

- 802.1x is compatible with the optional wireless network adapter, which provides secure wireless networking capabilities.

Details
Typically, 802.1x support is only leveraged for wireless devices. Most environments only support or require 802.1x authentication for network edge devices and for wireless connectivity. Lexmark's implementation of 802.1x supports wired and wireless environments.

Lexmark's 802.1x supports a wide array of network authentication methods:

- LEAP
- PEAP
- EAP-MD5
- EAP_MSCHAPV2
- EAP-TLS
- EAP-TTLS with the following authentication methods:
  - CHAP
  - MSCHAP
  - MSCHAPv2
  - PAP

The printer supports all of these protocols, and can be configured to include or exclude each protocol in the 802.1x protocol negotiation.

Device Hardening

Hardening a networked device is the process of securing the device's network interfaces. This includes eliminating unneeded or unused features and functions to prevent their abuse, locking down any interfaces that remain, and securing the data hosted by the device.

Lexmark's printers include a variety of mechanisms to facilitate in the device hardening process.

Port Filtering

Overview
Port filtering is implemented on Lexmark printers as a granular filter that allows network ports to be individually disabled. This allows the printer to be configured to meet virtually any policy regarding what protocols are and are not allowed on the network.

Benefits
Support for filtering individual ports provides a variety of benefits, including:

- Increased security by granular and authoritative control over the protocols the device processes or ignores.

- Cleaner port scans—shut down the unneeded ports and ports scans won't report potential vulnerabilities that need to be tracked down and understood.

- Redundancy—many protocols (such as HTTP, FTP, DHCP and others) can be disabled on the printer and port filtering allows the corresponding ports to be disabled as well.

- Reduced network traffic.

Details
The printer allows each of twenty five TCP and UDP ports to be individually opened or closed:

- TCP 21 (FTP)
- UDP 68 (DHCP)
- UDP 69 (TFTP)
- TCP 79 (FINGER)
- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 137 (WINS)
- UDP 161 (SNMP)
- UDP 162 (SNMP Traps)
- TCP 515 (LPR/LPD)
- TCP 631 (IPP)
- TCP 5000 (XML)
- TCP 5001 (IPDS)
- UDP 5353 (MDNS)
- TCP 8000 (HTTP)
- TCP 9000 (Telnet)
- TCP 9100 (Raw Print)
- TCP 9200 (IR Alerts)
- UDP 9200 (Discovery)
- UDP 9300 (NPAP)
- TCP 9400 (Lexmark Print Port)
- TCP 9500 (NPAP)
- TCP 9600 (IPDS)
- UDP 9700 (Plug-n-Print)
- TCP 10000 (Telnet)

Each port can be opened or closed, and when closed the printer will not generate or respond to traffic on the specified port even if the corresponding network application is otherwise enabled or disabled.

Hard Drive Encryption

Overview

A common concern for networked devices is that data will be exposed to remote access on the network. One avenue for this is through residual data: what if a system has appropriate protections for data while it's in use, but not when the data is no longer in use? Does leftover data remain on a system, and if so, is it less well protected than it should be?

Printers use hard drives for a variety of purposes, including to buffer print data while it is processed. It's important to assure that the buffered print data is well protected, to keep someone from accessing the potentially sensitive information contained in the print jobs that the printer receives.

Lexmark printers are equipped with the ability to encrypt the data on their hard drives, to protect it from external access at all times. When this feature is enabled, all data that's written to the hard drive is encrypted. This protects not only residual data from completed jobs, but protects data that's actively being used. This prohibits someone from powering off the printer in the middle of a job and making use of the data that was abruptly left on the drive.

Benefits

The benefits of hard drive encryption include:

- Increased security of active and residual data.
- The hardware-assisted encryption is applied in real time, so there's no delay for cleanup or post-processing after jobs have completed.
- A dynamically-generated encryption key stored on the printer (not the hard drive) makes the data on an encrypted drive useless on any other printer. Stealing the hard drive out of the printer doesn't yield access to the data it contains[2].

Details

By default, the data on the printer's hard drive is not encrypted. This does not mean that the contents of the drive are exposed, and there is no path by which residual data can be retrieved or accessed remotely[3].

When hard drive encryption is activated, the encryption key to be used (128 bit AES symmetric encryption) is pseudo randomly generated and stored in a proprietary fashion in the printer's memory. Note that the key is not stored on the hard drive itself, so if the hard drive is stolen from the printer the contents of the drive would remain indecipherable.

When the encryption function is activated, the hard drive is formatted and all data contained on the drive is lost. The encryption is then applied to all data placed on the hard drive, at all times.

TCP Connection Filtering

Overview

Lexmark printers support TCP connection filtering through their "Restricted Server List" feature. This feature allows the IP addresses from which the printer is to accept TCP/IP connections to be specified, and connections from all other addresses will be refused.

Benefits

Specifying a Restricted Server List includes the following benefits:

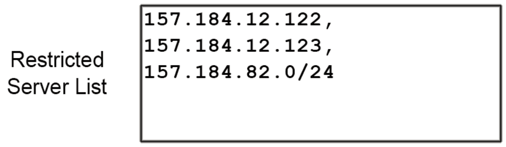
- Approved systems such as print servers and administrative workstations are allowed to make connections to the printer, so normal and approved functions such as printing and routine monitoring and maintenance occur normally.
- All network interactions that involve TCP/IP connections can be controlled, to increase security. The types of connections that rely on TCP/IP include HTTP/browser connections, FTP, telnet, and printing via LPR/LPD or through the Windows print subsystem. All of these connections will be allowed only to/from the specified systems.

[2] Note that this doesn't render the hard drive, itself, useless: when an encrypted hard drive is moved from one printer to another, it must be reformatted when it's placed into the new printer. The drive is portable, but the data on it is not.

[3] There are lots of factors that lead to this—more than are pertinent for this white paper. Briefly: there's no means by which to have the printer reprint or retrieve residual data, the printer doesn't support a network file system or file sharing, and there's no protocol supported by the printer that allows one to arbitrarily read or write data from the hard drive. So even without encryption of the hard drive's data, the disk drive contents are well protected.

- End user systems can be left off the list, which prohibits them from connecting to the printer (via a web browser, FTP, etc)—users are required to print through the print server, and are not allowed to configure or administer the system.
- Unknown systems would be left off of the list, which secures the printer against unauthorized external connections.

Details
The Restricted Server List allows up to 10 IP addresses or subnets to be specified. The printer responds normally to any address in the list, and rejects TCP connections to any address that's not in the list.



```
157.184.12.122,
157.184.12.123,
157.184.82.0/24
```

Comma delimited list of up to 10 IP addresses who are allowed to make TCP connections. Example: 157.184.195.0/24 is network prefix.

The Restricted Server List allows individual addresses and subnets to be specified. TCP connections from all other addresses will be refused by the printer.

The Restricted Server List does not affect UDP traffic, so connectionless interactions (such as a ping) are allowed from any address.

Secure Printing

Print data may be one of the most overlooked areas when it comes to network security.

Printed jobs routinely contain sensitive information—financial data, information that personally identifies customers or employees, account information, etc. Printers are commonly located in high-traffic areas with only basic physical security. In this environment, it's very easy for printed information to end up in the wrong hands, either accidentally or intentionally.

Lexmark printers include standard features that can substantially reduce this vulnerability.

Confidential Print

Overview
The Confidential Print feature addresses the basic concern of printed pages lying on the printer for anyone to pick up. With Confidential Print, the printer holds submitted jobs until the intended recipient is present at the device. By producing the printed job only when the proper PIN code is entered on the printer's operator panel, the job is delivered securely into the right hands.

Benefits
The features and benefits of Confidential Print include:

- An intuitive and effective means to deliver print jobs only when the recipient is at the printer.
- Security is provided with 4-digit PINs from 0000-9999—there are 10,000 possible values.
- The standard feature operates whether or not the printer is equipped with an optional hard disk. If no hard disk is present, the print job is held in the printer's RAM memory.
- If a hard disk is present, print jobs will be stored on the disk. This allows for more jobs to be held, and jobs will be retained of the printer is powered off. If Hard Drive Encryption is enabled (see page 7), the stored jobs will be encrypted for additional security.
- Unprinted jobs can be automatically purged after specified amount of time, to avoid a buildup of old jobs.

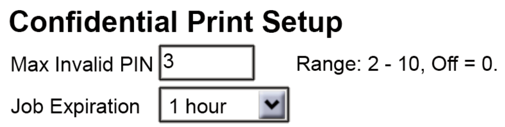
Details
Lexmark's printer drivers can be directed to submit Confidential Print jobs by specifying a Confidential Print PIN (Personal Identification Number). This is a standard feature of the printer drivers and of Lexmark printers.

When the printer receives a Confidential Print job, the data stream is stored on the printer's RAM

memory, or on the printer's hard disk if the hard disk option is present. Jobs stored in the printer's RAM memory will be deleted if the printer is powered off and can be deleted automatically by the printer if a memory shortage is encountered. For these reasons, it's strongly recommended that a hard disk be installed if Confidential Print is to be used extensively.

When a hard disk is present, jobs are retained across power cycles of the printer and the number of jobs that can be held by the printer is greatly increased.

Jobs stored on the printer's hard disk leverage the security of Hard Disk Encryption. Jobs stored in this way cannot be moved to a different printer on the hard disk; as discussed on page 7, encrypted hard drives cannot be moved from one printer to another without being reformatted.



Confidential Print Setup

Max Invalid PIN 3 Range: 2 - 10, Off = 0.

Job Expiration 1 hour

Setting a maximum number of invalid PIN entries thwarts attempts to guess PINs, and jobs can be set to expire after a range from one hour to one week.

For additional security, setting a maximum number of retries on PINs prevents brute-force attempts to guess PINs. If the PIN is entered incorrectly the specified number of times, the corresponding print job(s) will be deleted.

And, the Job Expiration feature allows jobs to be automatically deleted from the printer after a specified time interval, ranging from one hour to one week.

Printer Lockout

Overview

The Printer Lockout feature allows a printer to be put in a locked state where the operator panel doesn't allow any configuration, and incoming print jobs are stored on the printer's hard drive instead of being printed. This allows a printer to be secured during off hours: it can't be reconfigured via the operator panel, and print jobs won't be left sitting in the output bin.

The printer can be unlocked by entering a preconfigured PIN, at which time the held jobs will be printed and the printer resumes its normal operation.

Benefits

The features and benefits of Printer Lockout include:

- The printer can easily be secured during off hours.
- Jobs that are printed to a locked printer won't be exposed to being stolen out of the output bin.

Details

Printer Lockout is set up under administrative control, via the printer's embedded web page. A 4-digit PIN is specified, and that PIN can then be used to lock or unlock the printer, on its operator panel. This feature requires that a printer hard disk be present.

When the printer is locked, the operator panel does not allow any interaction other than specifying the PIN, to unlock it. While locked, incoming print jobs are not printed, but are stored on the printer's hard disk. If Hard Disk Encryption is enabled, then jobs stored on the hard disk will be encrypted.

When the printer is unlocked, the jobs that were received during the locked period are printed. If Confidential Print jobs are received during the locked period, those jobs are not printed, but are available through the typical Confidential Print jobs interface on the printer's operator panel.

IPSec for Secure Printing

In addition to securing the printed jobs as described by Confidential Print and Printer Lockout (above) Lexmark printers can protect the print data stream on the way to the printer. The IPSec capability described above can be used to establish a secure channel to the printer, over which encrypted print data can be transmitted.

By configuring IPSec between the printer and the networked print server, print jobs can be encrypted on their way to the printer. Independent of the printer configuration, IPSec or a similar mechanism

could be used to protect the transmission of the print jobs from the client workstations to the print server. This would create an end-to-end encrypted print path, for greater security.

Summary

Printer security is about protecting the printers, the network and the data that's involved in the use of the printers. Printer security is a complex issue with many elements to consider.

Lexmark's printers are equipped with an array of security features that allow you to secure networked printer devices and their use:

- Lexmark printers can be managed securely with device passwords, HTTPS, SNMPv3, and IPSec
- Lexmark printers can be hardened with Port Filtering, TCP Connection Filtering, and Hard Drive Encryption
- Lexmark printers support secure printing through Confidential Print, Printer Lockout, and IPSec

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to be, nor is it, a guaranty or warranty regarding the security of these products. This document is provided "as is" without any express or implied warranty. In no event will Lexmark have any liability for incidental, consequential (including lost profits), punitive, or indirect damages that may result from use or reliance on this document.