Lexmark

Secure by Design: Lexmark single-function and multifunction products

October 2020

Executive Overview

Lexmark multifunction products (MFPs) can be complex network devices that require security considerations. Lexmark MFPs, like other networked devices, include an array of security features and functions. Lexmark MFP security features and their benefits are described here. Lexmark single-function printers (SFPs) generally support many, if not most, of the same features as MFPs.

When connecting a device to your network, you must evaluate the security requirements necessary to ensure designed functionality, such as:

- How is the device protected from security risks?
- How is the device protected from unauthorized access?
- What makes an MFP secure when installing it on a network?
- What information does the device process? And what security considerations are related to that data?

Lexmark devices operate independently on networks, which means that, like networked computers and servers, they are capable of distributing sensitive information. The requirements for managing network access and for secure remote management are largely the same for MFPs and workstations. In other respects, however, the security considerations for MFPs are substantially different. MFPs do not run traditional operating systems. As a result, user authentication is applied differently. Furthermore, Lexmark MFPs do not share network files that need to be secured.

This document defines the major topics of the security of Lexmark devices and provides an overview of the security features and functionality that enable them to be deployed, managed and used securely on your network. For feature details for specific products, see “References” at the end of this document.

The features are organized into the following security areas:

- Secure Remote Management
- Secure Network Interfaces
- Secure Access
- Secure Data
- Solutions
- Secure Android Open Source Platform
- Security Standards

Secure Remote Management

To meet the demands of effectively managing a fleet of networked printers, Lexmark solutions-capable devices have the remote management security features you need—that is, they permit only authorized personnel to configure the device for network access.

Device and Settings Access

Overview

Changing device settings can be controlled through the use of function access controls (FACs), authentication and authorization mechanisms and the backup password. This keeps unauthorized users from altering the device’s settings, including security settings.

Lexmark devices support user authentication and authorization functions so that device administrators can select individual users and appropriate groups to make changes to a device based on a device's function and access rights. With this functionality, individual users, as well as users in a group, can use their network user name and password credentials to access devices. The device can determine whether a user has appropriate access based on the rights configured by the network administrator. This level of control applies to network access through the device's Web server, as well as to the configuration of the device through the control panel. For more details on authentication and authorization, see "Authentication and Authorization" in the "Secure Access" section of this document.

Additionally, Lexmark devices can be set up by the device administrator to have a backup password. This password provides access to the device's Security menu when it has limited or no access to network directory servers. The password is designed to give administrators access to the device so temporary changes can be made to the device's FACs.

Benefits

- Permit access control of device control panel functions.
- Specify who has the ability to configure devices using the Web page or control panel.
- Provide a secure method of access while the network is down.

Details

Device FACs are settings that can be configured to allow local and remote access to its functions and menus. Each of the device's functions and menus can be configured to use one of the following settings:

- No Security (default setting)
- Disabled (available if the function can be disabled)
- Restricted (via the authentication and authorization mechanism specified by a device administrator)

The device backup password can be created during the initial setup of the device and can be used in the event of limited or loss of network communication. The backup password provides global control over all Security menu settings. The backup password must be 8 to 128 characters in length. Passwords can include alphabetic, numeric and other characters to allow for substantial complexity. While the backup password enables an administrator to protect the device during the initial configuration of its security settings, it also provides local access to the device if network connectivity is lost.

While the backup password is used during initial device configuration or during the loss of connectivity of the device, the primary means of device access by users and administrators should be done via network user accounts (located on a corporate directory server) or local user accounts (located on the device). By requiring users and administrators to provide credentials for authentication, administrators can configure a device to determine access based on user and group needs. This access is done through a combination of FACs, authentication and authorization. For more details, see "Authentication and Authorization" in the "Secure Access" section of this document.

NOTE: The backup password is not associated with any accounts in the corporate directory. It is a password that is stored only in a device. This password should be shared only with those users who are authorized to modify the corresponding device's security settings.

Audit Logging

Overview

When you select Security Audit Log from the Security menu, Lexmark devices can track security-related events and device-setting changes. These actions can be exported to detailed logs that describe system user or activity events. The event-tracking feature proactively tracks and identifies potential risks and may be integrated with your intrusion detection system for real-time tracking.

Benefits

- Tracks device behavior and activities
- Identifies authenticated users, logging their activities

Details

The security-related events that are tracked are system-related events, setting changes, authentication and authorization events, disk-wiping events and real-time clock changes. Events that are logged include the following:

- IP address changes
- Logging behavior changes, such as not being able to send the logs to specific destinations or logging settings are changed
- Jobs started, canceled or completed
- Setting modifications of the embedded solutions' FAC
- Authentication or authorization success or failure events, including record of user identity
- Security reset by jumper changes
- Reset to factory defaults for settings, FACs and other device options
- Device settings modifications
- Creation, modification or deletion of authorization and authentication settings
- Kerberos file changes
- Authorization sessions created or modified
- Active Directory join or unjoin
- Certificates (device and certificate authority) added or removed
- Disk encryption, format and wiping
- IP Security (IPsec) connection failures
- Time-changed events
- Scan process events
- Embedded Solutions Framework (eSF) application events

NOTE: Events can also be logged by eSF applications.

Generated logs can be stored in the following ways:

- Stored internally in the device
- Sent to a remote syslog server in real time
- E-mailed to administrators
- Exported through the device Web page

Logs can also be digitally signed for security.

Digitally Signed Firmware Updates

Overview

Lexmark devices support a firmware download mechanism that enables the firmware that controls the device's behavior to be updated. This is a common feature among Lexmark products that is useful for feature upgrades or issue resolution. However, it is important that these firmware updates are carefully controlled to avoid any exposure to unauthorized code.

Benefits

- MFP capabilities can be maintained and extended through the application of authorized firmware updates.

- Unauthorized firmware packages and applications cannot be added to the MFP. If the code was not built and signed by Lexmark, the MFP rejects and discards the package.

Details

Lexmark devices inspect all downloaded firmware packages for a number of required attributes before the firmware is adopted or executed. The firmware must be packaged appropriately in a proprietary format. In addition, packages must be encrypted with a symmetric encryption algorithm through a key that is known only to Lexmark and is embedded securely in all devices. However, the strongest security measure comes from requiring that all firmware packages must include multiple digital 2048-bit RSA signatures from Lexmark. If these signatures are not valid, or if the message logs that accompany them indicate that the firmware has been changed since the signatures were applied, the firmware is discarded.

Firmware updates can be transmitted over the network so that devices can be updated all together simultaneously. This process can be automated and scheduled, and the process does not require someone to be present at each device. For security, the ability to perform this update over the network can be limited with access control restrictions to authorized administrators. Devices receive the code, validate it, adopt it and restart automatically. The process takes just a few minutes, and all the devices are available for use immediately.

Lexmark solutions-capable devices (those with touch-screen displays) support custom Lexmark eSF applications through an embedded-application platform. These applications must also be digitally signed by Lexmark before being adopted. This prohibits users from placing unauthorized applications on Lexmark devices.

Certificate Management

Overview

Certificate authority (CA) certificates are needed to allow a device to trust and validate the credentials of another system on the network. Without a CA certificate, the device has no other means to determine whether to trust the certificate that is presented by the system to create the secure connection.

Benefits

Certificates are the trust mechanism underlying much of public key infrastructure (PKI). A device's certificate management features support this trust from two viewpoints:

- Certificates enable devices to trust network services, guaranteeing the identity of the servers being accessed.
- Device certificates enable devices to be trusted by other network services if a trusted CA has signed the device certificate.

Details

Lexmark devices use certificates for HTTPS, SSL/TLS, IPsec and 802.1X authentications. Because they can be easily integrated with PKI environments, these devices can set up trusted communication transportation for 802.1X and IPsec certificate authorization for validating domain controller certificates and Lightweight Directory Access Protocol (LDAP), Secure Sockets Layer (SSL) or any other service that uses SSL or Transport Layer Security (TLS).

The device has a self-generated default device certificate by which the device can be uniquely identified. For some operations (for example, 802.1X and IPsec), the default device certificate needs to be upgraded to a certificate that has been signed by a CA so that other devices trust that specific device. A process is defined for upgrading the self-generated device certificate to one that has been signed by a known CA. For devices that are part of an Active Directory environment, this process has recently been simplified with an application installed on newer devices.

The Certificate Management menu is used for configuring printers to use device certificates for establishing SSL, IPsec and 802.1X connections. Additionally, devices use certificates for LDAP over SSL authentication and address book lookups. The configuring process for devices consists of the following steps:

1) Load the CA certificate for a certificate authority in the device.
2) Create a device certificate or use the device default certificate.
3) Create a CA-signed certificate with that device's certificate data using a certificate request file submitted to the CA.
4) Load the CA-signed certificate in the device.

NOTES:

- This process can be greatly simplified with a new Automatic Certificate Enrollment application, which is available when an Active Directory environment is used. For more details about the simplified process, see "Automatic Certificate Enrollment Application" in the "Solutions" section of this document.
- By default, Lexmark firmware generates 2048-bit RSA private keys and uses them to self-sign an X.509v1 device certificate. Current firmware uses SHA-256 hashing for signatures, while some older firmware might use weaker hash algorithms. The device private key is never externally accessible.

Some devices within Active Directory environments also support the ability to look for updated certificates at periodic intervals.

HTTPS

You can securely manage your networked printers and MFPs with HTTPS from each device's Embedded Web Server. For more security, you can use HTTPS to conveniently and effectively manage the device remotely.

Overview

The most common means to remotely configure networked devices, including Lexmark MFPs, is through the device's Web interface. You can configure device settings by pointing a browser to its IP address or host name and providing the proper credentials. However, browsers and the HTTP traffic associated with them are not inherently secure. An intruder can detect the network traffic used in the Web session and determine the device's password. To address this concern, Lexmark devices support HTTPS.

Through a recent firmware update, Lexmark has extended the capabilities of our devices' handling of HTTPS. This new capability allows a redirect from the HTTP (TCP 80) connection to a HTTPS (TCP 443) connection when using the devices' Embedded Web Server.

Benefits

The benefits of using HTTPS for Web sessions include:

- Ease of use in establishing a connection for the end user. Point the browser to "https://" instead of "http://" and the device and browser will automatically process the rest.
- The encryption of all data exchanged through the browser, including passwords and any oth er settings that are set or viewed.
- Supported by most commonly used Web browsers. HTTPS and SSL are widely used standards.
- Integration in preexisting CA or PKI environments. The device's certificate that allows the SSL session to be established can be signed by a CA.
- Web sessions can be conveniently and effectively secured.

Details

Lexmark devices include an Embedded Web Server. When a browser is pointed to a device's address with the "https://" prefix, the device and the client system negotiate an SSL connection. This involves the device passing its x.509 certificate to the client system to establish its identity. Because the device's certificate is self-signed by default, the client typically presents 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 does not receive further warnings.

Alternatively, the device's certificate can be signed by a CA. This can be an external CA or a CA that is internal to the customer's environment. The device'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 the HTTPS session. The HTTPS session is built on an SSL connection in which all exchanged data is encrypted. This protects the contents of the session against eavesdropping and enables secure remote management of the device.

NOTE: Device Web page access can be restricted to HTTPS only by turning off the HTTP port, leaving only the HTTPS port (443) active.

NOTE 2: Forced HTTPS redirection requires that both TCP port 80 and TCP port 443 be enabled in the TCP/IP Port Access menu.

SNMPv3

Overview

SNMP (Simple Network Management Protocol) provides another means to remotely configure Lexmark devices. Because SNMP can be used to both view and modify device settings, the basic security questions of how to control its use and how to protect the associated network traffic when it is used are relevant. Lexmark devices support the latest version of SNMP (currently SNMPv3). They also support SNMPv1 and v2 for backward compatibility. The standard protocol includes support for authentication and data encryption.

Benefits

With support for SNMPv3, Lexmark devices can be managed securely with standard SNMP console applications. There are two important elements to the security provided by SNMPv3:

- With authentication, authorized systems can see and manage devices through SNMPv3 while shutting out unauthorized systems.
- Encryption of the SNMPv3 packets protects the information from being detected while on the network, or more accurately, the detected data is useless because it is encrypted.

Details

Lexmark solutions-capable devices support SNMPv3. This protocol features extensive security capabilities, including the authentication and data encryption components for the secure remote management of a device. SNMPv1 and SNMPv2 are also supported.

Using the authentication features of SNMPv3, Lexmark devices can refute SNMPv3 traffic unless the requests are preceded by valid digital signatures, such as MD5 or SHA1. The device supports two SNMPv3 accounts. Authenticating against one yields the ability to read the device's settings but not write them; authenticating against the other provides the right to read and write the device's settings. Support for data privacy in SNMPv3 means that the device and SNMP client can use an encryption algorithm (DES, or AES with 128-, 192- or 256-bit keys) to encrypt the SNMPv3 traffic. Like other mechanisms for managing devices, SNMP can be disabled. If the protocol is not used in a particular environment, it can—and should be—turned off entirely.

NOTE: In order to utilize SNMPv3 securely, you need to disable SNMPv1 and 2, type a user name and password and select the minimum authentication level to "Authentication, Privacy."

Secure Password Reset

Overview

With the security reset feature, you can recover a device that is locked down through the use of one of the device's various authentication mechanisms. This feature can also be used if the administrator's password is lost or forgotten or the device loses network connectivity. You can use a cable lock to ensure that this is not reset maliciously.

Benefits

Provides a two-way method to recover a device if a local password is lost or forgotten, or if the device loses its ability to communicate with the network.

Details

The security reset feature requires the device administrator to set up the action of the security reset jumper. This setting can be found in the Security menu under Miscellaneous. There are two options that can be set on the security reset jumper:

- No Effect: If the security jumper is reset, there is no change to the device's security.
- Enable "Guest" Access: This is the default setting. This selection changes the device's FACs in the Security menu to No Security. It retains all authentication building blocks and security templates.

After the security reset jumper is selected, the device is ready for an unforeseen event, such as a lost password, forgotten password or a device loses its ability to communicate with the network. If such an event happens, the device administrator can access the device's controller board and move the reset jumper over to cover the middle and unexposed prongs as shown on the following image.

Secure Network Interfaces

Hardening a networked device is a powerful way to secure its network interfaces from malicious users. This includes blocking unnecessary features and functions, locking down any interfaces that remain and securing the data hosted by the device. Lexmark devices include a range of features embedded in the firmware to help you harden the device.

TCP Connection Filtering

Overview

Solutions-capable devices can be configured to allow TCP/IP connections only from a specified list of TCP/IP addresses, also known as whitelisting. This blocks all TCP connections from other addresses, protecting the device against unauthorized printing and configuration. Lexmark devices support TCP connection filtering with the Restricted Server List field. By using this option, the device can accept only previously specified TCP/IP connections and rejects all others.

Benefits

By specifying a restricted server list, you gain the following benefits:

- Approved systems, such as print servers and administrative workstations, are allowed to make connections to your device. This allows normal and approved functions, such as printing, routine monitoring and maintenance.
- 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 and browser connections, FTP, Telnet and printing through the Line Printer Remote/Line Printer Daemon (LPR/LPD) protocol or through the Windows print subsystem. All of these connections are allowed only to and from the specified systems.
- End-user systems can be omitted from the list, which prohibits them from connecting to the device through a Web browser or FTP connection.
- Any system that is not listed is refused access, securing the device against unauthorized external connections.

Details

The restricted server list allows up to 10 IP addresses or subnets to be specified. The device responds normally to any address in the list and rejects TCP connections to any address that is not on the list. The restricted server list does not affect UDP traffic, and so connectionless interactions, such as ping, are allowed from any address.

Port Filtering

Overview

You can gain more control over your network device's activity with port filtering, which you can use to easily configure your device to filter out traffic on specific network ports. Protocols such as FTP, HTTP, SNMP, Telnet and many others can be disabled.

Port filtering on Lexmark devices acts as a granular filter, which you can use to disable network ports individually. With port filtering, devices can be configured to comply with virtually any protocol network access policy.

Benefits

With support for filtering individual ports, you gain many benefits, including:

- Increased security. Provides granular and authoritative control over protocols the device processes or ignores.
- Cleaner port scans. By shutting down unneeded ports, the port scans do not report phantom vulnerabilities that need to be tracked down and understood.

Details

The device allows each of the following TCP and UDP ports to be individually opened or closed:

- TCP 21 (FTP)
- 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 9100 (Raw Print)
- PrintCryption
- UDP 9200 (Discovery)
- UDP 9300/9301/9302 (NPAP)
- TCP 9400 (Enhanced Print Port)
- TCP 9500/TCP 9501 (NPAP)
- TCP 9600 (IPDS)
- ThinPrint
- TCP 65002 (WSD Print Service)
- TCP 65004 (WSD Scan Service)

When a port is closed, a device does not generate or respond to traffic on the specified port even if the corresponding network application is enabled. It is good practice to close down any ports that you do not plan to use under normal operation by clearing them.

Lexmark has disabled and removed any configuration capabilities around Telnet due to the security risks associated with the protocol. In the rare cases that a customer requires Telnet (usually for legacy applications/utilities), Lexmark has the ability to enable the protocol on our solutions capable devices via a device license. The license is designed for specific devices to prevent the ability for a malicious user to enable Telnet on all Lexmark devices.

Lexmark devices do have flood protection capabilities to help limit device down time associated with DoS attacks. If the device determines that it is being attacked the device will conduct a soft reset on network connection and try to establish itself to a normal network operation.

NOTE: Not all ports are available in older devices.

802.1X

Overview

In virtually all network environments, you are required to log in to the network before you can send or receive e-mail, browse the Web or initiate other tasks. Increasingly, it is important to require devices, such as laptops or MFPs, to be authenticated before they can access networks. The protocol for this authentication is 802.1X, and Lexmark devices support the 802.1X protocol for device authentication.

Benefits

802.1X provides the following benefits:

- Enables the Lexmark device to authenticate itself on the network, increasing security.
- With support for a wide array of authentication methods, the 802.1 X authentication mechanism is 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

With 802.1X port authentication, devices can join wired and wireless networks by requiring authentication. You also have WPA-Enterprise security support when you use 802.1X port authentication with the Wi-Fi Protected Access (WPA) feature of an optional wireless print server.

Typically, 802.1X support is leveraged only for wireless devices. Most environments support or require 802.1 authentication only for edge devices and wireless connectivity. The Lexmark implementation of 802.1X supports both wired and wireless environments. The following network authentication methods are supported:

- LEAP
- PEAP
- EAP-MD5
- EAP_MSCHAPv2
- EAP-TLS
- EAP-TTLS with the following authentication methods:
    - CHAP
    - MSCHAP
    - MSCHAPv2
    - PAP

Lexmark devices support all these protocols and can be configured to include or exclude each protocol in the 802.1X protocol negotiation.

IPsec

Overview

IPsec is supported on Lexmark devices. This is an extremely important mechanism because it allows the device to establish a secure connection to other network nodes, such as print servers and management workstations. IPsec is available in conventional operating systems, such as Windows and Linux.

By applying IPsec between the device and a workstation or server, the traffic between these systems can be secured with strong encryption.

Benefits

IPsec can provide many benefits, including:

- Authorized systems can see and manage devices through SNMPv3, while shutting out unauthorized systems.
- The information is protected from being detected while on the network, or more accurately, the detected data is useless because it is encrypted when SNMPv3 packets are encrypted.
- Remote configuration by a Web session, Telnet, SNMP or any other IP-based means can be secured. Because mechanisms such as HTTPS and SNMPv3 can provide their own security, this provides a redundant level of security. Alternately, IPsec can be configured to be the only security mechanism, simplifying the security setup.
- All traffic between the Lexmark device management application, Mark vision Enterprise, and MFPs can be protected.

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

Details

IPsec safely sends information to your solutions-capable printers and MFPs by securing all network traffic to and from Lexmark devices with encryption and authentication. You can also protect the contents of jobs that are scanned to any destination, including servers running Lexmark Document Distributor, e-mail and network storage.

Lexmark devices support IPsec with pre-shared keys and certificates. IPsec can be used in pre-shared key mode and certificate mode, simultaneously. In pre-shared key mode, printers and MFPs can be configured to establish a secure IPsec connection with up to five other systems. Lexmark devices and these systems are configured with a passphrase, which is used to authenticate the systems and to encrypt the data subsequently.

In certificate mode, Lexmark devices can be configured to establish a secure IPsec connection with up to five other systems or subnets. In this configuration, printers and MFPs can exchange data securely with a large number of systems, and the process can be integrated with a PKI or CA infrastructure. The use of certificates provides a more robust and scalable solution, without the burden of configuring or managing keys or passphrases.

Lexmark devices can store and apply two certificates for use with IPsec. Each device 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 is embedded in a printer or MFP and available through its Web interface. With this certificate generation, a device's identity can be validated by other systems in the CA environment. In addition, the device can store the CA's certificate as a trusted root CA certificate so that it can validate the identity of other systems in the CA environment.

Secure Network Time Protocol

Overview

Network Time Protocol (NTP) provides devices with a common time source to keep them synchronized with the correct date and time so they can successfully use any authentication method that requires accurate time. To ensure that the date and time are being delivered only from an approved authenticated time source, Secure NTP is also supported.

Benefits

Secure NTP provides the capability for devices on the network to obtain their time from an authenticated, secured source.

Details

Lexmark devices support the use of Secure NTP, which is used for clock synchronization of various devices on the network. This complements audit logging to prevent date and time changes and simplifies several authentication methods that rely on accurate time settings.

Secure NTP uses MD5-encrypted keys to authenticate the time stamps that come from the time server. These keys are agreed on in advance between the printer and the time server. If a time stamp comes to the printer from the server without the correct key, the printer ignores the time stamp.

Fax and Network Separation

Overview

A common question about networked MFPs is “Are they exposed to intruders with the presence of a fax modem?” The concern is that an intruder can dial in to the MFP through the fax modem and manipulate the device or somehow gain access to the network to which it is connected.

The reality is there is no exposure through a fax modem or network access on Lexmark MFPs. With the fax modem on Lexmark devices, only the exchange of facsimile images is possible. There is no path by which the fax modem connection can interact with or control the MFP’s network interface, and there is no facility to configure the MFP’s settings through the fax modem connection. With the Lexmark fax modem connection, you can send and receive only fax images.

The fax modem connection is restricted to Facsimile Class 1 mode, and the data transferred over the modem is limited to facsimile image data only. The connection is not the same as on a laptop or other device modem where an arbitrary network connection can be established through the fax modem. Rather, the information exchanged over the MFP’s modem is restricted to image data only.

Network protocols are not supported through the fax modem. There is no support for exchanging TCP/IP traffic of any sort, including FTP, HTTP, SNMP, Telnet or any other form of network packet. Also, there is no support for modifying an MFP’s configuration through the fax modem connection. Settings cannot be viewed or changed, and there is no access to an MFP’s file system through the fax connection.

Benefits

Support for fax on a networked MFP includes the following benefits:

- Incoming fax images can be printed as hard copy or routed to a predefined e-mail, FTP or workflow destination. This does not undermine the network’s security because the incoming data can only be in an image format. The fax connection cannot receive or transmit executable data such as applications, scripts or viruses.
- Incoming faxes can be redirected to an alternate fax machine. This can be useful when an office is temporarily closed, as it allows incoming faxes to be forwarded to an alternate device that is being regularly monitored.

Details

There is a long list of reasons why the presence of a fax modem on a Lexmark device with a network adapter does not expose security. This document explores each of these points in more detail:

- There is no support for controlling the device through the phone connection. You cannot dial in to the device and interact with it through FTP, Telnet or similar mechanisms.
- The modem and network adapter hardware are on separate cards and cannot communicate directly with one another. This prohibits data from moving between the two channels.
- The modem is configured to send and receive fax only, not data.
- The modem’s configuration is limited and controlled by the MFP’s firmware. The MFP firmware does not allow arbitrary data to be exchanged over the fax modem; only facsimile data representing page images can be exchanged.

- The avenues by which the MFP's firmware can be updated are secured. Plus, unauthorized firmware and software cannot be loaded in the MFP.

All these factors prevent the interaction of the fax modem and network adapter hardware from exposure to security threats.

No control of the device through phone lines

Many devices that support an analog phone modem can be controlled remotely through the phone line. On such devices, you can call the device and interact with it: turn it on or off, change its settings and so on. Typically, this is managed through something such as Telnet. However, the presence of an analog phone modem does not automatically involve any such mechanism. For the device to allow such interaction, the support needs to be built in and intentionally provided. Lexmark products do not include or allow this kind of control.

No Lexmark device allows any sort of configuration through the phone line. There are no diagnostic modes by which any external mechanism can control or reconfigure the behavior of the modem. The only data that the analog phone modem is capable of exchanging is fax information. It does not allow for configuration or any sort of remote control of the device, and it does not allow any avenue to access the network to which the device is connected.

Modem and internal network adapter are separate by design

Lexmark MFPs use a third-party fax chip to handle analog-to-digital processing, while the rest of the fax modem process is handled directly by Lexmark firmware. The internal network adapter function is implemented separately from the modem capabilities, and the two functions are implemented on separate circuit cards. The fax processes are handled directly by the Lexmark firmware, as is the network adapter interaction. Additionally, the Lexmark firmware is designed to prohibit direct interaction between the fax and network components.

Modem is configured for fax only

Control of the fax functionality is incorporated directly into the Lexmark firmware. The fax chip that sends and receives data over the phone line is directly controlled by the Lexmark firmware. The modem chip is in a mode that is even more restrictive than Class 1 mode, and it relies on the Lexmark firmware for composition and transmission of fax data. The firmware explicitly blocks the transmission of frames in data mode and allows only sending and receiving facsimile jobs.

No support for the PS fax mechanism

Some fax devices employ a mechanism known as PS Fax or PostScript File Transfer. When two fax devices support PS Fax and connect through an analog phone session, PS Fax enables a print job to be transmitted in its original PostScript format. This is faster and produces higher-quality output than converting the job to a bitmap at the sending end and transmitting the bitmap. However, the ability of the receiving device to accept non-image data exposes the device to security threats. The PostScript job itself can potentially include malicious functions, and the support for opening the connection for non-image data can leave the device vulnerable to other types of transmissions. For these reasons, the PS Fax capability is not supported on Lexmark MFPs.

Phone lines do not provide way to update firmware

Because the only way to change the behavior of the modem is to modify the firmware, how that might be accomplished is a reasonable concern. Because the network connection is secure, the concern is the phone line because it is connected to the outside world. The nature of the Lexmark firmware and the modem's fax operation, however, is to accept only fax frames—frames that contain image data. When these frames are combined, they are assembled and wrapped in PostScript commands and submitted to the MFP's interpreter as image data. There is no other data path available, and no way for data that comes through the fax to be treated as anything but a fax image. If the data that is received does not represent an image, the data is purged as an invalid PostScript job. There is no avenue by which modified firmware (or any sort of executable code) can be packaged as a fax job and become operable in a Lexmark device.

Secure Access

Network scans and printed documents that routinely contain sensitive information—such as financial data, customer or employee identification and account information—are often overlooked when it comes to network security. Lexmark devices include standard features that can substantially reduce the security risk by ensuring that only authorized users have access to the data.

Authentication and Authorization

Overview

When you select a function such as Scan to E-mail, the MFP can require you to authenticate yourself before proceeding. This limits device access to valid users only and enables the MFP to identify who is performing the function.

Lexmark devices support not only user authentication, but authorization as well. This allows device administrators to grant individual users and appropriate groups the right to access a particular device function or functions, while restricting other users or groups from using the same functions. With this capability, individual users or group members are able to use their network user name and password to access the device. The device can determine whether the user has access to the appropriate functions, based on the access rights configured by the device administrator. This level of control applies to network access through the device's Web server, as well as to the configuration and use of the device through the touch-screen interface. You can also configure the device to authenticate and authorize users against internal accounts, passwords and PINs—as well as against a corporate directory through an encrypted channel. These authentication methods are secure over an SSL channel and are compatible with Active Directory and other directory-server platforms.

An important aspect of user authentication and authorization is that you can enter your normal, or corporate, user ID and password. You should not, and do not, need to remember a special set of information to use a Lexmark device. Instead, the device makes use of the corporate directory to validate your credentials against the standard, centralized database.

Benefits

The benefits of user authentication and authorization include:

- Securing an MFP by limiting who can use its control panel to access functions such as Copy, Color Copy or Scan to Network.
- Anonymous e-mail is avoided by inserting the identity of the authenticated user in e-mail generated by the Scan to E-mail function. With additional configuration, the Scan to E-mail function can also limit e-mails to a predetermined destination (for example, someone@ourcompany.com) so that e-mail cannot be sent to arbitrary destinations.

- When network authentication is used, you authenticate your identity by using your normal user name and password, just as if you are logging in to your workstation or laptop. This keeps the process simple and intuitive.
- Faxes sent with networked fax servers can automatically send an e-mail confirmation of the fax to the sender's e-mail, because the MFP recognizes who is sending the fax.

Details

The process of authenticating users is flexible. Lexmark devices can use a variety of internal authentication mechanisms and network directory authentication mechanisms and protocols to validate user credentials. Lexmark devices can be set up to use device internal accounts, device passwords, device PINs, LDAP (with or without SSL/TLS), Kerberos, LDAP+GSSAPI and NTLM for authenticating users.

Support for a wide array of authentication protocols means that the device user authentication function is compatible with an array of network environments, including Microsoft Active Directory, Novell eDirectory and other directory environments that support LDAP. Secure user authentication protocols, such as LDAP with SSL/TLS configured, Kerberos, LDAP+GSSAPI and NTLM, protect users' credentials during the authentication process.

The device manages authentication and authorization with one, or more, of the following methods:

- PIN or Panel PIN Protect
- Password or Web Page Password Protect
- Internal accounts
- LDAP
- LDAP+GSSAPI
- Kerberos 5 (used only in conjunction with LDAP+GSSAPI)
- Active Directory

To provide low-level security, you can use either PIN and Password or Panel PIN Protect and Web Page Password Protect for some printer models, by limiting access to a printer—or specific functions of a printer—to anyone who knows the correct code. This type of security might be appropriate if a printer is located in the lobby or other public areas of a business so that only employees who know the password or PIN are able to use the printer. Because anyone who enters the correct password or PIN receives the same privileges and users cannot be individually identified, passwords and PINs are considered less secure than other building blocks that require you to be identified, or both be identified and authorized.

NOTE: The default settings do not contain any authentication or authorization building blocks, which means that everyone has unrestricted access to the Embedded Web Server.

Access controls

With more than 50 access controls, you can choose from a list of available security templates to control local and remote access to specific menus and functions and workflows. You can even disable functions entirely. Examples of walk-up functions that can be controlled are:

- Copy
- Scan to E-mail
- Scan to Fax
- Scan to FTP
- Print held jobs (such as confidential print jobs)
- The ability to print jobs from a portable USB memory device (for example, a flash drive)
- The ability to scan jobs to a portable USB memory device
- USB device access
- Launching embedded applications

Access to applications that are installed on the device can also be restricted.

Local and remote access to a number of different administrative menus can also be managed with access controls. Examples of menus that can be controlled are:

- Security menu
- Settings menu
- Network/Ports menu
- Configuration menu

Device management functions can also be restricted with access controls. Examples of device capabilities that can be controlled are:

- Firmware updates
- Control panel lock
- Web importing and exporting of settings
- Remote management

Access to these functions can be set by selection of a permission for that function. For more information, see the Embedded Web Server - Security guide for your particular device.

Active Directory

Overview

Microsoft Active Directory support is provided on solution-enabled Lexmark devices (those with touch-screen displays). Using Active Directory for the latest generation of Lexmark touch-screen devices is a secure method of authentication and authorization that is also simpler to set up and easier to manage device security. Active Directory authentication is provided by Kerberos and authorization by LDAP+GSSAPI.

Active Directory is also supported in solution-enabled devices; however, the level of support is different. On some devices, the device is supported as a resource with device credentials (a device service account) while on others the device support is similar to a computer (a security principal).

Benefits

The benefits of using Active Directory are:

- Simplify network setup and PKI enrollment
- Automatically create and configure LDAP+GSSAPI and Kerberos authentication building blocks
- Enhance fault tolerance with automatic detection of multiple domain controllers
- Get certificate chains from the domain controller by automatic download
- Support single sign-on sharing of authentication credentials

Details

With Active Directory, the joining process is greatly simplified. To join, you access the device Web page through HTTPS and enter a few required settings (domain name, administrator user name and password). The setup process is complete. The required LDAP+GSSAPI and Kerberos setup is completed automatically using data from the Active Directory domain controller. The enhanced Active Directory support sets up the device using computer credentials, which creates a more secure connection because the IT administrator does not need to issue or manage device service accounts.

Because the Kerberos file is internally generated with additionally discovered Active Directory environmental information, there is better affinity and reliability.

Additional key distribution centers (KDCs) in the environment are included in the file and accessible, if required. This also permits devices to use the optimum selection from the domain controllers detected in the environment. The device automatically downloads domain controller CA certificate chains and will maintain this (if certificate monitoring is specified) by periodically verifying that the certificate chain is up-to-date.

Active Directory participation permits the usage of single sign-on. If already logged in to the Active Directory environment, the device Web page access can use Integrated Windows Authentication to automatically and securely authenticate the user, for example, using card reader authentication for device Web page access.

For the latest firmware updates, the process is further simplified so that you can select automatic setup of additional security services from the Active Directory joining screen.

- If the LDAP address book is selected, the LDAP server address book information is configured with Active Directory server data.
- If Standard Admin Groups and Security Templates is selected, then a security template called admin is selected with all permissions and a security template called Active Directory is automatically generated, ready to use. You need only to select Access Controls and apply the desired access restrictions for the Active Directory user.
- If CA Certificate Monitoring is selected, then the CA certificates that are obtained f rom the domain controller are monitored for updates.

Some other devices also participate in Active Directory environments, but they use device credentials, not computer credentials. The devices connect with the Active Directory server specified, but they do not search for the optimum server. A Kerberos file is created (but not retrieved from the domain controller server), and LDAP+GSSAPI authentication is automatically defined. The domain controller CA certificate chain is not automatically downloaded.

Secure LDAP

Overview

When scanning to e-mail or scanning to fax, you can select the recipient's e-mail address or fax number rather than manually typing it. This important convenience is made possible through LDAP. With LDAP, an MFP can query the corporate directory for information. The use of SSL protocol adds security to the process. By establishing an SSL connection before generating LDAP queries, an MFP and the directory server can protect the information they exchange.

Benefits

The benefits of using LDAP over SSL include:

- The information queried by an MFP is secured (encrypted) on the network.
- MFPs can leverage your existing PKI infrastructure to perform SSL, conforming to your standard security practices.

Details

All LDAP traffic to and from Lexmark devices can be secured with TLS/SSL to preserve its confidentiality and privacy. LDAP information that is exchanged over a TLS/SSL connection, such as credentials, names and e-mail addresses and fax numbers, is encrypted.

MFPs can be configured to trust a customer's CA by installing the CA's X.509 certificate on the MFP. Multiple CA certificates can be installed to establish trust to more than one CA. MFP configurations dictate that the MFP precedes all LDAP traffic with the negotiation of an SSL connection. The directory server provides its certificate, the MFP validates it and a secure encrypted communication channel is established. All subsequent LDAP traffic moves over this channel, so all LDAP information is encrypted on its network. This applies to LDAP queries for e-mail and fax information, as well as LDAP-based user authentication.

Auto-insertion of Sender's E-mail Address

Overview

When you select a function on an MFP, such as Scan to E-mail, the MFP can require you to authenticate yourself (that is, log in) before proceeding. At the same time that the device is authenticating you, the device is also querying your information and automatically inserting your e-mail address in the From field of the e-mail. By automatically populating the From field of the outgoing e-mail, you are identifying yourself to the e-mail recipient.

Benefits

Anonymous e-mail is eliminated by inserting the identity of the authenticated user in the e-mail generated with the "Scan to E-mail" function.

Details

Auto-insertion of e-mail addresses is a form of nonrepudiation by automatically querying the authenticated user's information and inserting his or her e-mail address in the From field of an outgoing e-mail. Lexmark devices can use a variety of protocols to validate and look up user information: LDAP, LDAP over SSL, LDAP+GSSAPI or Active Directory. Using any of these authentication protocols enables devices to not only authenticate but also to query that same user information in the directory server. If the device locates the user's e-mail address, it populates the From field with the user's e-mail address. The user can then use the "Scan to E-mail" function. If the device cannot locate the user's e-mail address, the device does not allow the user to proceed with the function.

Login Restrictions

Overview

Lexmark devices can restrict the number of failed attempts that a malicious user can use to try to gain access to a device with a false password. This capability can help reduce the risk associated with password attacks on user accounts. In addition to restricting the number of invalid login attempts, the device can be configured to require a set period of time before allowing users to retry access attempts. These tools are especially useful if the customer environment does not have an identity management service capable of locking down user accounts after multiple failed attempts.

Benefits

Benefits gained from login restrictions on Lexmark devices are:

- Mitigates risks associated with brute-force attacks on user passwords by reducing the number of login attempts
- Specifies a minimum time before any additional password entries may be accepted

Details

You can inhibit password attacks by restricting the number of failed login attempts within a specific time frame. Also, imposing a lockout time before additional logins are permitted after login failures further inhibits attacks. Additionally, after a valid user is logged in to the device, inactivity timers are enforced to ensure that users are logged out in a timely manner. In conjunction with restricting login attempts and lockout time, the device can be set up to utilize the audit capabilities to track what user account is being attacked, the time and date of the attack, the frequency of the attack and the devices where the attacks occurred.

Control Panel Lock

Overview

With the control panel lock feature, you can place a Lexmark device into a locked state so that the control panel cannot be used for any user operations or configuration. It cannot copy or scan jobs. It cannot be reconfigured with the control panel, and incoming jobs do not sit exposed in the output bin. If the device has a hard disk, incoming print and fax jobs are stored in the hard disk instead of being printed. The device can be unlocked by entering authorized user credentials, at which time the held jobs are printed and the device resumes its normal operation.

Benefits

The features and benefits of the device lock feature include:

- Devices can be secured with a simple method so that during off hours, scanning and printing operations are not permitted.
- Jobs printed to a locked device cannot be stolen from the output bin.

Details

The control panel lock is configured by creating an authentication building block and applying it against the control panel's Lock function access control through the device's Embedded Web Server. Depending on the type of authentication building block and the security template that is applied to this function access control, you can enter a device PIN, a device password or network credentials to lock or unlock the device at its control panel. This feature requires the installation of a hard disk.

When a device is locked, the control panel does not allow any interaction other than specifying the appropriate credentials to unlock it. While locked, incoming print jobs and faxes are not printed, but stored in the device's hard disk. If hard disk encryption is enabled, then jobs stored in the hard disk are encrypted.

When the device is unlocked, jobs received during the locked period are printed. Any confidential print jobs received during the locked period are not printed, but they are available through the typical "confidential print job" interface on the device's control panel.

Confidential Print

Overview

The Confidential Print feature addresses the basic concern of printed pages left on the device for anyone to pick up. With Confidential Print, the device securely holds submitted jobs until the intended recipient is present at the device and enters the proper PIN code on the device's control panel.

Benefits

- Ensures that jobs are only printed when the authorized recipient is at the device
- Operates whether or not the device is equipped with a hard disk

Details

Lexmark device drivers can be directed to submit confidential print jobs by specifying a confidential four-digit print PIN. This is a standard feature on Lexmark devices and drivers. When a device receives a confidential print job, the data stream is stored in the device's random access memory (RAM) or in the device's hard disk. Jobs stored in the device's RAM are deleted if the device is turned off. Jobs stored in RAM can also be deleted automatically by the device if a memory shortage is encountered. For these reasons, it's strongly recommended that a hard disk be installed if the Confidential Print function is to be used extensively.

When a hard disk is present, jobs are retained across power cycles of devices, greatly increasing the number of jobs that can be held by Lexmark devices. Jobs buffered to a device's hard disk can leverage the security of hard disk encryption. Buffered data on an encrypted hard disk cannot be processed if that hard disk is moved to another device. Furthermore, the hard disk itself cannot be used by another device without being reformatted.

For additional security, setting a maximum number of retries on PINs prevents brute-force attempts to guess PINs. If a PIN is entered incorrectly after the specified number of times, the corresponding print jobs are deleted. Additionally, with the Job Expiration feature, your jobs can be automatically deleted from the device after a specified time interval, ranging from one hour to one week.

Secure Internet Printing Protocol

Overview

Secure Internet Printing Protocol (IPPS) protects Internet Printing Protocol (IPP)-based print jobs and printer queries by providing SSL data encryption and user authentication.

Benefits

IPPS provides the following benefits:

- Encryption for all IPPS traffic
- Forced user authentication to use IPPS

Details

IPP is a standard protocol, operating over TCP port 631, which makes it possible for clients to query a printer's capabilities, submit print jobs and query device and job status. To secure this potentially confidential data, the IPPS protocol is available. It can be enabled by setting the Internet Printing Protocol function access control (available under the "Management" heading on the Access Control page) to an existing security template.

After IPPS has been enabled, connecting clients are upgraded via the unencrypted connection to SSL/TLS on port 631 and are required to be authenticated before any further communication is permitted. Communications are encrypted before authentication to protect credentials, and all IPP traffic is SSL encrypted.

Incoming Fax Holding

Overview

With the Incoming Fax Holding feature, MFPs can receive faxes and hold them until they are released. Devices with a hard disk can be configured through a scheduling menu to temporarily store received faxes rather than immediately print them. These held faxes are secured until the designated release time has elapsed or proper credentials have been entered on the Lexmark device. This ensures the fax output is not being exposed to unauthorized persons during off hours.

Benefits

Some benefits of Incoming Fax Holding are:

- Determines when faxes are automatically printed or held for authorized release
- Secures fax output to prevent use by malicious individuals

Details

The Incoming Fax Holding feature is enabled on the Fax Holding menu. This is where the device administrator can turn the capability on or off, or specify a schedule of when to hold faxes and when to print them. Setting up the schedule data is uncomplicated: The administrator selects a command, such as Print Faxes or Hold Faxes, and then selects the time at which the action occurs and the days the action should happen (for example, after work hours and weekends).

For added security, the device administrator can require a user or a group to be authenticated prior to releasing the faxes. By adding this component, the administrator is validating that the faxes are released to authorized individuals and audits the action (for example, who released the faxes and the date and time) if there are concerns about malicious use.

Secure Start Process and Operating System Protections

Overview

Security is an integral part of the Lexmark development process and is the reason security is a standard offering on all Lexmark devices. Device security should not be an afterthought or a separate security chip inserted in a device after it has been manufactured. Device security should be holistic, which includes protection against malware and viruses. This is why Lexmark has been committed to developing security mechanisms around device operating systems, firmware updates and embedded solutions well before it became a published attack vector for malicious individuals.

Benefits

Secure starting processes and operating system protections offer several benefits:

- Ensures that there is virtually no option for loading malware or viruses in the operating system or other operating firmware of a device
- Ensures that only trusted firmware is installed on Lexmark devices by using digital signatures and other security mechanisms
- Stops operation and reports error if self-checking detects its security is compromised

Details

For their operating systems, Lexmark devices use a version of Linux. The kernel, which is a central part of the Linux operating system, is obtained directly from the Linux distribution site and not from a third party. Lexmark makes modifications to the Linux kernel so that the operating system can better meet the needs of hard copy devices. This approach provides hardening against external attacks:

Additional protections used in the development of the Lexmark operating system are:

- Standard applications, such as Apache, Samba, Telnet, FTP and so on, that are found in a standard Linux distribution, have well-documented security exposures and are subject to rootkit attacks. These applications have been removed and replaced with applications specifically written by Lexmark developers for a hard copy device.
- Lexmark development teams create custom applications that control functions such as print, fax, copy and scan.

- After all modifications are made to the operating system, it is firewalled and hardened to the point that the embedded environment is closed.
- In the event that a vulnerability is found on a device or additional functionalities are added to the operating system, the entire operating system is replaced on the device through a firmware update.

Only trusted firmware can be loaded on a Lexmark device. The following requirements are defined so that significant protections are provided with the device firmware:

- The data must be packed appropriately in a format that is specific to the device type.
- The data must be encrypted so that it is decrypted correctly with a symmetric key. This key is embedded in the device's firmware during manufacturing. To create a software package that passes the requirements of Lexmark devices, an individual must have this symmetric key. This is not published, nor can it be extracted from Lexmark firmware.
- The data (after decryption) consists of multiple sub-packages, each of which must have a separate digital signature. The digital signature provides two protections: It validates that the firmware came from Lexmark and that the firmware has not been modified since it was created.
- Firmware updates can be restricted to authenticated and authorized users or disabled through the device access function controls.

The chain-of-trust process developed by Lexmark to check and validate the integrity of a device's operating system during startup, normal operation and execution of an internal application is defined in the following list. If any of the following tests fail, the device halts operation of all processes and reports an error.

- The device's physical hardware is used to validate the secure bootloader, which is then used to verify the signature on the kernel.
- The kernel is then used to verify the signatures on each firmware flash partition before it is mounted by the device.
- Internal device drivers and executable code are designed to be operated on trusted read -only flash partitions. No code is ever written to a standard or optional device hard disk.
- Each time a block is paged from the trusted flash memory to RAM, its hash value is verified by the kernel, which provides continuous verification and tamper detection.

Other protections that Lexmark has in place to protect the device's operating system are as follows:

- Device usage data is placed in tamper-proof memory so that it can be analyzed in the event that the device is compromised.
- All hard copy devices use non-x86 processors.
- The device does not accept incoming e-mail, nor does it contain its own SMTP server or service.
- The device hard disks (standard or optional) are not designed to be long-term storage devices, nor do they allow users or administrators to load or extract information, create folders, share, or create a network file share or FTP information to the hard drive.
- The device does not allow incoming remote procedure calls (RPCs), which limit the propagation of malware from other devices.
- The device does not recognize or run files with executable extensions. Image files, such as BMP, DCX, GIF, JPEG, JPG, PCX, PDF, PNG, TIF, TIFF and XPS, are recognized as print-related data.

eSF Application Security

Overview

Lexmark devices can be extended with the Lexmark eSF. Included in Lexmark devices is an execution platform in solution-enabled devices that permits function enhancements to devices through the loading and running of custom applications. These applications are loaded, configured and remain resident on the device, extending the capabilities of the device. To ensure that device security is not compromised, well-defined interfaces are specified, an application certification process is specified and secure encrypted, signed application install packages are created.

Benefits

- Device functions are enhanced by installing eSF applications in a secure manner using signed, encrypted files that are verified by the device before installation.
- Device function usage by eSF applications is restricted to well-defined APIs.

Details

In the same way that Lexmark devices inspect all downloaded firmware packages for a number of required attributes before the firmware is adopted or executed, eSF applications are delivered to devices using the same packaging as Lexmark device firmware. The application must be packaged appropriately, that is, in a proprietary format. In addition, packages must be encrypted with a symmetric encryption algorithm through a key that is known only to Lexmark and is embedded securely in all devices. However, the strongest security comes from the requirement that all application packages must include multiple digital 2048-bit RSA signatures from Lexmark. If these signatures are not valid, or if the message logs that accompany them indicate that the firmware has been changed since the signatures were applied, the application is discarded.

Lexmark eSF applications can be transmitted over the network, which allows all devices on that network to be updated efficiently. This process can be automated and scheduled, and does not require someone to be at each device. The device receives the application, validates it, adopts it and stores it automatically.

For security, the ability to install, update or remove applications can be limited. First, eSF flash files are subject to the same firmware update access control as other firmware update flash files, so if this access is disabled, eSF applications cannot be installed except through the Embedded Solutions setup page of the Web user interface. Access to the Web page can be limited with access control restrictions to authorized administrators.

The security of the application also relies on a secure development and certification process to verify that the operation of the application performs the desired function and does not permit malicious malware or viruses, or does not allow undesired behavior. Most eSF applications are developed by Lexmark developers, but even for those that are developed by third parties, the completed application is verified for acceptable behavior and adherence to device and memory access restrictions. Only after approval is the application packaged and signed by Lexmark for distribution.

Protected USB Ports

Overview

USB ports on personal computers provide a means to connect devices of various types for 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 devices provide the following:

- Detect an inserted USB mass storage device (such as a flash drive) and display, by name, the image files and/or flash files that are stored in the device.
- Select a supported image file for printing or select a valid flash file to initiate a firmware update (if permitted by security settings).
- Scan data directly to the USB flash drive.
- Access can be permitted or restricted based on a defined schedule.

If enhanced security is required, the device can limit or not permit these operations, or not permit any use of USB devices.

The USB host ports on Lexmark devices do not permit 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 data stream files
- The submission of any other sort of data (executable code, configuration files and so on)
- Recording any sort of data from the printer to a USB-attached device other than jobs that are a direct scan to a USB flash drive
- 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 (except in cases where the device is configured to use the USB port for authentication using a smart card)

Disabling the front USB port is an option at manufacturing or by the device administrator during setup for recent devices using access control restrictions. Some Lexmark devices also have a rear USB host port. The use of this port is restricted to card readers and HIDs, such as a keyboard.

Benefits

The benefits of restricting the functions of portable USB memory devices include:

- Carefully control environments where sensitive documents exist by not permitting users to perform scan-to-USB operations.
- Do not permit users to perform print-from-USB operations in environments where printing is tracked or allowed only on a fee basis.
- Limit the ability to perform scan-to or print-from USB devices to only authenticated users.
- Do not permit just any USB memory device to use highly restricted environments.
- Eliminate virus and malware attack options.
- Restrict when the USB ports are available for usage.

Details

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

The purpose of the USB host port on Lexmark devices is to allow convenient printing and scanning of image files, to permit attachment of card readers for authentication and authorization purposes and HIDs, such as keyboards, and to access fast, easy maintenance activities through firmware updates for technicians.

The supported image file formats are BMP, DCX, GIF, JPG, PCX, PDF, PNG, TIF, TIFF and XPS. 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 the following:

USB support is limited

When a USB device is connected to a USB host port (such as on the front of a Lexmark laser printer or MFP), 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 support only devices that enumerate with a mass storage device class and HID for simple input devices (for example, keyboards and authentication card readers) and specific chip card interface device (CCID) card reader devices used for authentication. This means that if a device, such as a USB network card, is inserted, the printer does not establish a connection to it. USB flash drives are a typical example of the sort of device you might expect to use with Lexmark devices. These devices are widespread 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, so they are likely to be recognized and compatible with Lexmark devices. If a USB device does not meet these requirements, then the printer or MFP rejects the external device. One other supported device is the Lexmark wireless adapter. This device is uniquely recognized by the enumeration process and accepted by a Lexmark printing device.

Support is limited to printing image files, direct flash drive scanning and updating firmware through flash files

When a USB flash drive is inserted in a 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 (BMP, DCX, GIF, JPEG, JPG, PCX, PDF, PNG, TIF, TIFF and XPS) and firmware files (FLS) on the device. No other type of file is displayed or supported. Files that contain PostScript or PCL data streams are not supported. When you decide 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 that file's format. Also, firmware files are accepted on the device only if 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 load executable code in the printer by storing it in a file called, for example, *HarmlessJob.pdf*.

Image files are treated internally, just as if they were submitted to the device through any of the other device ports (parallel, network and so on). This means that the USB host port does not provide any avenues for submitting data that did not already exist.

In many regards, the USB host port is less forgiving because the printer decides whether to display and allow the submission of data through the USB connection. Unlike other connections, the printer determines what can be sent to it through the USB port.

There is no support for submitting executable code, code updates, configuration changes or anything other than BMP, DCX, GIF, JPEG, JPG, PCX, PDF, PNG, TIF, TIFF and XPS files to the printer through the USB port.

Another method for printing image files that are supported for some devices is printing from digital cameras that support the PictBridge connection. There is no way to import files using this connection. The only result that can be obtained is printing of image files that are resident in the camera or in the device for those devices that support PictBridge. If the device does not support PictBridge or the camera is not supported, an error message is displayed.

No support for startup from USB-attached devices

On many personal computer systems, the USB host port is included in the list of partitions that can be used for startup; that is, you can potentially start such computers from a flash drive. However, this is not permitted with Lexmark devices. The USB ports are not included in the startup sequence.

No support for network interaction with USB-attached devices

A USB-attached device cannot exchange data in any way with the network to which the device is attached. 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 is cases where the printer or MFP provides authentication capabilities through an HID, such as a card reader for card-based authentication. In this instance, an embedded application is installed through the Lexmark eSF 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. Limited text character input from standard USB keyboards is permitted with the HID interface, but this input is routed and used only as a substitute for the on-screen keyboard as supported for devices with touch screens.

No support for adding additional drivers or functionality

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

Firmware updates—which are supported through the USB device port on the back of the printer or MFP and through the network interface—must include multiple digital signatures. This ensures that the printer or MFP accepts only code that is produced and provided by Lexmark. 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

In some environments, controlling the submission of print jobs (including image files) is important, and all uncontrolled avenues by which jobs can be submitted are undesirable. For example, in a college library, there might be a system by which users can submit print jobs over the network and then be charged for the pages they print. In such a case, it is unacceptable to let users walk up and submit jobs to the printer from a USB flash drive.

You 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 cannot be reactivated by the device administrator or end user under any circumstances.

On recent devices, the device administrator can disable the port through the security access controls menu on the device's Embedded Web Server. In this case, the port can be enabled, again, at a later time, if required. The function of disabling or enabling the port can be restricted so that end users cannot re-enable the port.

Lexmark devices support portable USB memory devices (flash drives) to be used for scan-to-USB or print-from-USB tasks. Printer or MFP configurations cannot be set or recorded with USB devices. The ability to scan-to or print-from USB devices can be controlled separately by a particular authentication building block and security template, or set independently to any of the following states:

- No Security: The functions are active and no authentication is required. This is appropriate for environments where no control or tracking is necessary.
- Disabled: The device does not permit print-from or scan-to USB devices.

NOTE: For some devices, you can stipulate that no USB memory device can be used with the “Allow Flash Drive Access” access control selection.

Secure Data

Lexmark has defined mechanisms and processes to protect the data on permanent memory devices and allow the secure permanent removal of data when it is no longer required.

To meet today’s complex printing requirements, Lexmark devices are equipped with non-volatile memory to store essential system information when the devices are turned off. Some Lexmark devices can also be equipped with a hard disk to buffer jobs or collate large jobs, or store forms, fonts or macros. To run some printing applications or printer software solutions, a hard disk is required. The use of non-volatile memory and hard disks are industry-standard methods for enhancing the performance of print and imaging devices.

Hard disks on Lexmark devices are designed for device-specific functionality and are not designed, nor can be used, as long-term storage for items unrelated to printing and scanning. The basic architecture of these devices does not have the capability for users to extract information, create folders, share the hard disk, and create a network file share or FTP information to the device’s hard disk directly from a client device.

The device hard disk is primarily designed to store print or image data, font data, forms data, macros and, in some cases, job data. In addition, Lexmark uses hard disks for temporarily buffering the scanning, faxing and copying of data. In general, print-related data is processed in RAM unless the job exceeds the amount of RAM on the device or if you select the Confidential Print or Print and Hold feature, which is enabled through the printer driver. These devices feature controls that help secure data when it is stored or passed through the hard disk. Plus, they block malicious users from gaining physical access to the hard disk.

Hard Disk Encryption

Overview

A common concern for networked devices is that data is exposed to remove access. For example, what if a system has appropriate protections for data while it is in use by not when the date is idle? Does unused data remain on a system, and if so, is it less protected than it should be?

Lexmark devices use hard disk drives for a variety of purposes, including buffering scanned data during the course of copy jobs and buffering print data during print jobs. It is important to ensure that the buffered data is well protected so no one can access potentially sensitive information contained in image scans or print jobs that the device receives.

Lexmark devices can encrypt all data on hard disks to protect it from external access at all times. When this feature is enabled, all data written to a hard disk is encrypted. This protects not only residual data that remains after printing jobs, but it also protects data actively being used. This prohibits someone from turning off the device in the middle of a job and making use of the data left on the disk.

Benefits

The benefits of hard disk encryption include:

- Increased security of active and residual data
- No delay for cleanup or post-processing after jobs are finished because hardware-assisted encryption is applied in real time
- The encrypted data is device specific and is not transportable

Details

By default, the data on the device's hard disk is not encrypted. This is sufficient protection for most threats because there is no device functionality enabling remote access to the data. Disk encryption protects against the threat of removing the hard disk from the SFP or MFP, and attempting to gain access to the data it contains from another device.

When hard disk encryption is activated, the encryption key to be used (256-bit AES symmetric encryption) is pseudo-randomly generated and stored in a proprietary fashion in a device's memory. The hard disk is then reformatted with the encryption key. Any data on the disk is lost. Notice that the key, which is unique to the device, is not stored in the hard disk itself. So, if the hard disk is removed and placed in another Lexmark device with hard disk encryption enabled, the hard disk attempts to verify its encryption key with the other device's encryption key—and it fails.

Because the verified encryption key on the hard disk is different than the device's encryption key, the device identifies the failure and asks you to reformat the hard disk with a new encryption key, destroying the existing encrypted data on the hard disk. When the encryption function is activated, the hard disk is formatted, and all data on the disk is lost. The encryption is then applied to all data placed on the hard disk at all times.

Non-volatile Memory Wipe

A non-volatile memory wipe erases a printer's memory. Lexmark devices use two forms of non-volatile memory—EEPROM and NAND. These components store the device operating system, device settings, network information, embedded solution applications, various scanner settings and bookmark settings. No user-related print, copy or scan data is stored in non-volatile memory.

Overview

The printer memory erasing function ("Erase Printer Memory," "Wipe All Settings," "Erase all apps and app settings," depending on the device model) deletes all content stored in the various forms of flash memory on your device. You can completely clear all settings, solutions and job data on the device. This function is ideal when retiring, recycling or removing a device from a secure environment.

Benefits

Some benefits of a non-volatile memory wipe are:

- Device settings are restored to original factory ship selections, removing any setting values that may be incorrect.
- Printer memory erasing enables a complete reset, which permits movement and reinstallation at another location with no residual settings retained.

Details

The “Erase Printer Memory” (“Wipe All Settings”) function is a tool for erasing all contents stored in the various forms of non-volatile memory on a device. “Wipe All Settings” is accessed on a device’s control panel in the Configuration menu. “Erase Printer Memory” is accessed via the device’s Web page in the Restore Factory Defaults menu (for later EC devices) or the Maintenance menu (for new devices). It is also included in the Out of Service Wiping (Out of Service Erase) function, which is described in “Out of Service Wiping” later in this section. Using “Erase Printer Memory” (“Wipe All Settings”) completely clears all device settings, including network and security settings. Installed applications and their settings are removed. (Applications shipped with a device remain, but their settings are reset.)

The latest line of Lexmark devices allows more granularity for clearing the device’s non-volatile memory. The user can select the following options from the Erase Printer Memory function:

- Erase all printer and network settings
- Erase user flash
- Erase all apps and app settings

NOTE: After all settings are removed or reset, network connectivity cannot be retained because the device is in the out-of-box shipping state. You are prompted to restart the device or turn it off for transport. There is no network connectivity until the device is restarted to ensure that the original ship configuration is maintained.

Lexmark Secure Element

Overview

Lexmark’s Secure Element is an optional security component that is designed to enhance and protect the generation and storage of encryption keys used by a Lexmark device.

The Secure Element is a customer installable option or can be installed/shipped with the product at manufacturing. The Secure Element is essentially a smart card that installs in a Lexmark device’s controller board in the same manner as a SIM card which can be found in mobile phones.

This technology grants additional layers to secure and highly capable Lexmark devices by enhancing its ability to protect the cryptographic keys that are generated by and installed on the device. In addition to providing a more secure key store, the Secure Element provisions the device with a method to generate cryptographic keys faster and with more complex random numbers.

Benefits

The Secure Element is designed to strengthen a Lexmark device’s ability to secure information whether it is stored in the device or transmitting critical information to/from a device. The main purposes of this component is to provide improved capabilities to secure the cryptographic keys that are generated by the device and provide more complex methods to generate random numbers which are used to create cryptographic keys. A major benefit is that this card will immediately satisfy many corporations/government agencies that need to have certifications around the device’s cryptography.

- Stronger random number generation.
- Secure key store for certificates and encryption keys.
- Hard disk encryption key is protected by Secure Element.
- Secure Element will be a requirement for future Common Criteria and FIPS PUB 140-2 validations.

Hard Disk File Wiping

The file-based disk wipe sanitizes the portion of the hard disk where job data was stored after a job has been processed so that no residual data can be read. “Complete,” “Out of Service” or “Sanitize all information on hard disk” disk erasure, which is explained later, erases the entire disk while the file-based disk wiping described in the following paragraph erases the portion of the disk where the job data was stored. Lexmark devices offer a single-pass or multiple-pass wipe that is compliant with the National Institute of Standards and Technology (NIST) and U.S. Department of Defense (DOD). You can perform this operation in several ways.

Overview

Lexmark uses hard disks on devices to temporarily buffer scan, fax, print and copy data that exceeds the amount of RAM installed on the device. Buffered data can be deleted from the device’s hard disk immediately after an original scan, fax, print or copy job is complete, or at other times as specified. Additionally, devices can temporarily hold print jobs on a hard disk if you use the Confidential Print and Print and Hold features when fax jobs are received and sent. This data remains on the hard disk until you print or delete the job, or until the document expires through the job expiration feature.

When a data file is deleted from a hard disk, the data that is associated with that file is not actually deleted. This data remains on the hard disk and, theoretically, can be recovered with substantial effort. Lexmark devices support an additional mechanism for protecting residual data—hard disk file wiping. Hard disk file wiping actively overwrites any job data files that are deleted. You have a choice of single or multiple passes of data, which removes all data residue from the deleted file.

With some Lexmark devices, you can select when hard disk file wiping is activated (automatic, scheduled, manual) while others automatically delete a file permanently, immediately after it is no longer required for printing, scanning and so on. Disk wiping erases only job data from a device’s hard disk that is not currently in use by the file system. All permanent data on the device’s hard disk is preserved, such as downloaded fonts, macros and held jobs. The Lexmark wiping process adheres to NIST and DOD (DOD 5220.22-M) guidelines for overwriting confidential data.

Benefits

The benefits of hard disk wiping include increased security of residual data.

Details

The settings available for hard disk file wiping are Automatic, Scheduled and Manual. Off or Do Not Start Now is the default setting. Disk wiping for these three methods can be either single or multiple pass. Single-pass and multiple-pass settings determine the number of overwrite passes that are used during the wiping process. Highly confidential information should be wiped only with the multiple-pass method. Multiple-pass wiping takes longer than the single-pass version because more overwrite passes are used.

NOTE: Automatic, Scheduled and Manual wiping selections are available only if a formatted, non-defective device hard disk is installed.

Automatic

Immediately overwrites areas of the disk that were used for job processing. Automatic wiping marks all disk space used by a previous job and does not permit the file system to reuse this marked space until it has been sanitized. Automatic wiping is the only wiping process that operates without having to take the device offline for the duration of the wiping process.

NOTE: Automatic wiping is the preferred method of wiping because the time that job files are resident on the disk is minimized. Automatic wiping is the only option that is defined for a number of devices and is the default.

Scheduled

Enables you to select when the disk wiping of previous job files is executed. When the disk space that is used for a job is no longer required, it is marked for wiping later. At the first available non-busy time period after the next scheduled-time setting, the device goes offline and begins the disk wiping process for any marked disk space. No user warning or confirmation message is displayed. Both the Manual and Scheduled settings enable the file system to reuse marked disk space without wiping it.

Manual

Immediately starts wiping all disk space that is marked as space previously used for job data. The device is offline during the wiping process. Do Not Start Now (also on the menu) is the default setting. The disk-wiping menu can be accessed from the device's Embedded Web Server for all devices that support a hard drive or the device's control panel for most devices. If the disk-wiping access control is activated, then you must be successfully authenticated and have the required authorization to initiate disk wiping.

Single- and Multiple-pass Disk Wiping

Each disk-wiping method (automatic, scheduled, manual) can use either a single- or multiple-pass wipe. Single-pass wiping only replaces the data with zeros, whereas multiple-pass wiping includes more methods of sanitation. Multiple-pass wiping, used with automatic, scheduled or manual mode, is currently defined to meet NIST/DOD/DOE standards for confidential data (DOD 5220.22-M, Section 8-306).

Complete Hard Disk Erasure

Overview

As indicated above, "Complete" or "Sanitize all information on hard disk" hard disk erasure wipes clean the entire hard disk. You should perform a complete hard disk erasure process before a device is removed from any current location. This function is different than those previously described. With the "Sanitize all information on hard disk" (also called "Complete Wipe Disk" or "Erase Hard Disk") command, you can eliminate all contents of a disk.

Benefits

- Eliminating the need to remove or process the hard disk before the device is retired, recycled or otherwise removed from a secure environment
- Completely removing all residual customer data from the hard disk

Details

There are several circumstances where Lexmark recommends that you erase the memory installed in your Lexmark device, including when the device is:

- Decommissioned
- Having its hard disk replaced
- Being moved to a different department or location
- Being serviced by someone outside your organization
- Being removed from your premises for service

You can use the "Sanitize all information on hard disk" command (also called "Complete Wipe Disk" or "Erase Hard Disk") from the Configuration menu (or remotely from the device Web page for most devices). Within this menu, the user may select single-pass and multiple-pass erasure, which will erase the hard disk using the same algorithms as for file wiping. Multiple-pass erasure is currently defined to meet NIST/DOD/DOE standards for confidential data.

Depending on the product or EC version, the selections are called Wipe Disk (Fast) and Wipe Disk (Secure) or Single Pass and Multi-Pass or Single Pass Erase and Multiple Pass Erase. When initiating the process, the device is removed from service until the erasure is completed. Erasure progress is displayed. On later firmware versions the time remaining for completion is displayed while the erasure proceeds.

Out of Service Wiping

With the Out of Service command, you can use the functions of Wipe All Settings and Complete Hard Disk Erasure (Wiping) in one step when removing a device from service or removing it from a secure environment. To ensure that no customer data remains on the device hard disk, Lexmark recommends that you use both Wipe All Settings and Complete Hard Disk Wiping commands. With the Out of Service command (available on later firmware updates of most devices), you can choose to initiate both of these functions at the same time from either the Configuration Menu or from the device Web page.

Benefits

- Provides a simplified process to prepare the device for removal from service or a secure environment

Details

For later firmware both the Out of Service wiping function is available on the device Web page. This selection is visible only if security is enabled (any basic security or advanced security selection), and Security Menu Access Control has been set to use that security template (any setting except No Security). For later firmware update releases this function (called Out of Service Erase) is updated and included on both the Configuration Menu and the device Web page (as part of the Restore Factory Defaults menu). In the updated version, the predicted time for the disk erasure is displayed before the process is initiated, and the time remaining before erasure is completed is displayed while erasure is in progress.

Physical Lock Support

Overview

Lexmark devices support cabled computer locks, which you can use to physically secure the devices' critical and sensitive components, such as the controller board and hard disk.

Benefits

Some benefits of physical lock support are:

- Protects against malicious access to the devices' critical components, such as the hard disk, controller board, optional memory (flash or RAM), fax modem and network card
- Reduces the threat of a hard disk drive being stolen from a device

Details

One of the most forgotten parts of a secure-device strategy is to protect assets from physical theft. Most IT departments inventory and apply asset tags to their hard copy devices, but rarely do these same departments lock down their hard copy devices with physical locks. Some of these devices contain hard disk drives that buffer printing- and scanning-related data. In addition to buffering data, hard disk drives (and optional flash memory) can be used to store fonts, forms, fax data and so on. Lexmark devices can protect this data with wiping and encryption technologies. Adding a physical lock to a device gives the device administrator added confidence, knowing that the devices' critical components are protected so that only authorized individuals have access to these components.

Solutions

Lexmark products support installable solutions that are written to utilize the eSF platform in the device. These solutions extend the basic capabilities of the device, often enhancing the security of the device or the customer environment.

Print Release Application

Overview

With Lexmark Print Management, employees send print jobs from anywhere—including their desktops, tablets or smartphones—and then release the jobs for printing whenever and wherever they're ready. This means confidential information stays protected, and print jobs don't pile up unnecessarily on office printers.

All documents are held in a print queue until their owners release them. The queue can be hosted on premise or in the cloud so that you can take advantage of additional features and benefits. Documents can be released at any enabled device, whether the device is located across the room, in another building or thousands of miles away. To release your documents, swipe your ID card or type your credentials at the device, and then select the documents you need to print.

Benefits

The benefits of the Print Management feature are:

- Determines when documents should be automatically printed or held for authorized release
- Deletes unprinted documents from the print server after a set period of time to prevent draft documents from being seen by unauthorized persons
- Can be integrated with enterprise identity systems for secure authentication
- Restricts printing of draft documents with confidential information
- Increases flexibility for employees
- Strengthens access controls to improve security and compliance
- Scales easily with on-premise, secure cloud or hybrid deployment

Details

This solution consists of an externally hosted document management application and a device resident application which provides the local user interface to permit selection and release of the desired print jobs.

Certificate Automatic Enrollment Application

Overview

The Certificate Automatic Enrollment application is operational only for some solutions-enabled devices. Creating a CA-signed device certificate to permit establishing SSL, IPsec and 802.1X connections is normally a lengthy process (which follows). When the device is present in an Active Directory environment, this application significantly simplifies the process, requiring entry of only a limited number of domain control and user identity parameters.

To create a CA-signed device certificate using the traditional manual (without the ACE application) process:

1) Load the CA certificate for a CA in the device.
2) Create a device certificate (or use the device default certificate).
3) Create a CA-signed certificate (using device certificate data) using a certificate request file from the device that is delivered to the CA.
4) Load the CA-signed certificate in the device.

Benefits

The benefit of the application is the ability to automatically generate and retrieve a CA-signed device certificate.

Details

After installation, the application automatically creates device certificate signing requests and passes the signing request to the CA for approval. It then retrieves the CA-signed device certificate and installs the certificate. The manual process is replaced by an easy-to-use process with only limited initial setup required (entry of minimal Active Directory information).

NOTE: For this application to function, the device must be joined to an Active Directory environment, and a Certificate Enrollment Web Services (Server Role) application needs to be installed on the CA server in the Active Directory environment.

Secure Held Print Jobs Application

Overview

Secure Held Print Jobs is an easy-to-use application that prevents the accidental exposure of sensitive or confidential business information by holding jobs at the device until an authorized user releases the job for printing.

Benefits

Benefits of the Secure Held Print Jobs application are:

- Holds documents until they're released by an authorized user
- Releases print jobs whenever you're ready
- Reduces expenses related to print output
- Enables DRAM wiping of job data when enabled

Details

The Secure Held Print Jobs application uses a four-digit PIN or ID card to prevent unauthorized access to documents, keeping them safe and secure. This helps stop sensitive company information from being left in an output tray or picked up and viewed by an unauthorized person.

You can send and store jobs in the printer and release them at your convenience. There's no need to interrupt what you're doing to pick up a document. You can also review a document before printing multiple copies. Make sure jobs are deleted after the documents are printed, and set up the job to print as many copies as you need. You can even have the job expire at intervals ranging from one hour to one week.

By decreasing the number of unclaimed documents left in your company's output trays, you can achieve significant cost savings. Also, when enabled by selecting the Clear Print Data setting, all DRAM that is used to store job data is automatically cleared after the job is completed.

Contactless Card Authentication Support

Overview

Lexmark devices support a number of different contactless card solutions (applications) for basic badge authentication where your identity is linked to your ID badge. The badge authentication solutions verify the badge ID and retrieves your user information so that it can be used for accessing held print jobs, identifying the source of scanned documents, or identifying you for other identification purposes.

Benefits

The benefits of contactless card authentication are:

- Ease of use
- Use existing physical ID badges for logical access to the device
- Does not require a complete Active Directory PKI smart card infrastructure

Details

Lexmark badge authentication solutions are designed to work with card reader driver application solutions. The card reader driver solutions provide card ID data to other solutions that manage workflows or access to device functions. For details, refer to the individual application solution descriptions.

Lexmark devices support a number of different card readers and card types. The recommended reader for most badge types is the OMNICKEY 5427CK. The 5427CK supports HID Prox, HID iCLASS, MIFARE and HID Indala cards.

The following readers are supported with the eSF keyboard reader application. Only the USB keyboard variant of these readers is supported. For supported card types of each reader, refer to the reader manufacturer specs:

- Elatec TWN3
- Elatec TWN4
- RF IDeas pcProx
- RF IDeas pcProx Plus (RDR-80581AKU only)

Additional keyboard emulation readers are supported on a per-customer basis when requested. Magnetic stripe cards are supported with the following readers (driver application not required):

- MagTek 21040102
- MagTek 21040107
- MagTek SureSwipe 21040145

CAC/PIV and SIPRNet Card (Authentication)

Overview

The Common Access Card (CAC) and Personal Identity Verification (PIV) authentication solution provides safe workflow processes throughout federal government operations by providing more control over the security of networked Lexmark devices. Digital-information-capture functions require strong user authentication to protect against unauthorized access and guard critical data. The same solution also supports Secret Internet Protocol Router Network (SIPRNet) token cards (using a different card interface application) to provide access over the SIPRNet. Lexmark enables this robust authentication by preventing the use of network functions at Lexmark devices until the user's credentials have been authenticated. For enhanced network security, it encrypts all network traffic, including electronic documents and paper-based data. It also creates a secure, easy-to-use interface.

Benefits

Some of the benefits of CAC/PIV/SIPRNet authentication are:

- Delivers flexible and easy configuration function for administrators
- Holds confidential print jobs until released by an authorized recipient
- Validates a card through Active Directory or Online Certificate Status Protocol (OCSP) for Tumbleweed or CoreStreet

Details

The Lexmark solution ensures that only authorized employees can access the network through its devices, giving government agencies another option for enhanced network security protection. Users cannot initiate workflow processes at locked devices without first inserting a CAC/SIPRNet card and obtaining authentication. Because the user's identification is associated with all functions initiated while the CAC/SIPRNet card is in the reader, an audit trail can also be created to track user activity.

Using the user's credentials from a CAC/SIPRNet card enhances the Scan to E-mail workflow by providing a more secure, personalized experience. E-mail addresses can be found without the need for a service account. Outgoing e-mail is addressed with the user's account information, eliminating anonymous e-mail. S/MIME support is available for enhanced security and privacy. CAC/SIPRNet credentials can be used to log in to an exchange server through SMTP to validate user authorization prior to sending e-mail. The Lexmark CAC/SIPRNet solution has a rich set of customization capabilities so that only authorized users have access to specific workflows. Global restrictions can be set up so that all users can print jobs and copy and fax normally without CAC/SIPRNet authentication, requiring only authentication for scanning and other network functions. Users can also be organized by Active Directory groups so that function access is available only to those who are authorized.

The Lexmark CAC/SIPRNet solution for SFPs and MFPs follows the same protocol as current laptop and PC CAC authentication processes. The onboard CAC/SIPRNet reader and user-friendly e-Task MFP touch screen makes authentication simple and secure:

1) Insert your CAC/SIPRNet card in the MFP's card reader. You are prompted to enter your PIN.
2) The MFP validates the PIN against the CAC/SIPRNet card. It then extracts the PKI certificates from the CAC/SIPRNet card and sends them to the Windows domain controller for validation. The domain controller response can be validated at the MFP or against an OCSP responder or repeater.
3) When the card is validated, the MFP home screen appears, and user preferences and other system parameters are also implemented. You can then perform any of the MFP functions, such as Scan to E-mail (digitally signed and encrypted), Scan to Home (or Other) Network Folder, Scan to Document Management System and so on.

By leaving the CAC/SIPRNet card in the reader, no additional login is required to perform additional MFP functions. You remain logged in as long as your CAC/SIPRNet card stays in the reader; removing your card returns the MFP to its locked, secure state.

NOTE: Lexmark PIV authentication meets all current Homeland Security Presidential Directive-12 (HSPD-12) standards.

Lexmark Contact Authentication Device

Overview

The Lexmark Contact Authentication Device provides enhanced control access to network printers and MFPs with secure authentication at print release. The device easily connects on the front of the printer or MFP and instantly provides a more secure environment for your business. The device's carefully engineered features enhanced security and prevents unauthorized users from gaining access to sensitive information.

With a single touch, administrators can use the Lexmark Contact Authentication Device to manage access to devices and authorize access to specific functions including e-mail, fax, copy or scan. Plus, the device provides full compliance with all major industry standards and works seamlessly with virtually every contact smart card.

Lexmark Contactless Authentication Device

Overview

The Lexmark Contactless Authentication Device provides enhanced access to network printers and smart MFP's with secure authentication at print release. The device easily connects on front of the printer or MFP and instantly provides a more secure environment for your users and your organization.

Administrators can use the Lexmark Contactless Authentication Device to manage access to devices and authorize access to specific functions including e-mail, fax, copy or scan, all with a single touch. Plus, the device provides full compliance with all major industry standards and works seamlessly with virtually every contact smart card and PC operating system.

Secure Document Monitor

Overview

Lexmark Secure Document Monitor helps reduce the risks and liabilities associated with security breaches of physical documents. This single solution can simultaneously monitor and audit the information in millions of documents coming from all of your SFPs and MFPs to improve the way your enterprise detects, investigates and deters wrongdoing.

Benefits

Benefits of Secure Document Monitor are:

- Tracks every document that is printed, copied, scanned or faxed through an output device
- Audits and monitors previously inaccessible information to check for leaks
- Helps facilitate compliance with government and industry regulations
- Adds powerful monitoring capabilities to your system at a lower cost

Details

Lexmark Secure Document Monitor creates a searchable digital image file of every document that passes through your supported Lexmark devices. This includes print jobs that you send from your computer or mobile device, documents that are scanned or copied and incoming and outbound faxes.

These digital images are stored with related metadata, such as device, user and location, preparing them for document auditing. Lexmark Secure Document Monitor gives you the option to launch forensic searches based on keywords or phrases (full-text search), document attributes (who, what, when and where the event occurred) and even search text in graphics, illustrations and photos. With the proactive Discovery Alerts feature, which continuously searches content as it passes through the system, you are automatically notified if any keywords or phrases are found.

Information sent to Lexmark

At Lexmark, we are committed to delivering the best possible experience for our customers and are always looking for opportunities to improve our award-winning product line.

We rely on customer feedback to make our products the best they can be. This lets us understand the device's performance to help us drive future innovations in product design and service.

Sending information to Lexmark is a simple and easy way to provide feedback. However, no information will be sent to Lexmark unless you give Lexmark permission to do so. If you choose to participate, your device will periodically send Lexmark an ANONYMOUS summary of its usage, performance, device interaction and/or session information depending upon which information you choose to share.

Information is sent to Lexmark over your Internet connection. You can choose to start or stop sending information at any time. Different printer models and different firmware versions have the ability to send different types of information.

There are up to four types of information:

- Supplies and page usage information, such as the number of pages and toner levels. This helps Lexmark better understand how customers use our products.
- Device performance information, such as device errors and metrics. This helps Lexm ark understand device performance and enable a higher level of service. (Sharing device performance information also enables sharing supplies and page usage information as described in #1 above).
- Device interaction information, such as op-panel sequencing, button presses, and session timing. This helps Lexmark understand user behavior, improve device performance and enable a higher level of service. (Sharing device interaction information also enables sharing supplies and page usage information and device performance information as described in #1 and #2 above).
- Session information - activities performed by users on the device. There are 3 setting options for session information: (1) or no user ID information, (2) generic user ID information, (3) actual us er ID information. Sharing session information is an independent setting from the selections for sharing the information in #1, #2, and #3 above.

More details about information collected is available in at the end of this document – Information sent to Lexmark table.

Secure Android Open Source Project

Lexmark has moved to using Android Open Source Project to drive the graphical user interface (GUI) for the next line of Lexmark touch-screen devices. In doing so, there will be concerns as to the security of devices that run a software stack that is installed in millions of phones and tablets. The following sections outline known Android security risks and how Lexmark is addressing these issues to provide system-wide security to Lexmark devices and customers who use them.

User as Administrator

Android users can install applications, grant application permissions, download data and access unprotected networks—the user can reign free over their Android domain without restriction.

Lexmark Security Measures

Lexmark devices have their own internal security subsystem outside of Android that will secure the device and prevent users from accessing the device to install applications, download data and so forth.

Google Play

Google's verification processes for applications entering their market have been shown to be woefully lacking over the last few years, leading to a number of malware-infected applications and games being made illegitimately available to users.

Lexmark Security Measures

Lexmark does not, and does not plan to, support installing applications directly from Google Play. Since Lexmark has its own application distribution system, Lexmark will leverage this system to distribute applications.

Application Permissions

In the form of a pop-up, users may see these notifications as a nuisance, a delay in accessing a newly downloaded application, or they may simply not understand the nature of the requests. Common permissions that could raise an eyebrow would include "Read/Send SMS," "Access/Find Location," "Access IMEI," "Phone ID," "Brick" (required to disable the device in trace and wipe applications), "Access Camera" and so on. Such requests may be integral to functionality, but could equally be integral to recording calls and transmitting sign-in credentials.

Lexmark Security Measures

Lexmark does not support installing applications from Google Play. Only Lexmark authorized applications can be added to the device; if the application cannot be digitally verified, it will be rejected and discarded. Additionally, the Lexmark security subsystem will secure the device from users accessing the device and downloading data.

Malicious Application Injections

Data/process transfers between virtualized application environments are handled by a protocol of implicit and explicit intents. Transmission or interception of an intent by a malicious application can result in data being compromised as the target application will respond to the string, potentially resulting in data loss.

Lexmark Security Measures

Lexmark does not support installing applications from any source other than the Lexmark application distribution system. Additionally, the Lexmark security subsystem will secure the device from users accessing the device and downloading data.

Third-Party Applications

In a rapidly growing operating system environment, it can be difficult to identify reputable vendors, especially considering the nature of the Android community. Even reputable services can allow their mobile applications to transmit sensitive data without encryption, despite their existing security measures for Web application versions.

Lexmark Security Measures

Lexmark does not support installing application from any third-party vendors via Google Play. Additionally, the Lexmark security subsystem will secure the device from users accessing it and downloading data. This is done by authenticating via digital signatures; only appropriately authenticated signatures are accepted.

Direct Connect to PC

HTC devices (e.g., smartphones) are increasingly using applications, such as “Go to Meeting” and “TeamViewer,” for remote access. Although secured, these third-party services still provide a line into the corporate network and may be implemented fairly easily on to an endpoint.

Any Android device can be connected to a PC via a USB cable, exposing the contents of its SD card for read/write/delete access. The SD card itself, as removable storage, can also be easily accessed. These methods could be utilized themselves for bringing malware into a corporate network, for downloading malicious content onto a PC or uploading data as soon as it is connected.

Lexmark Security Measures

The current USB devices do not connect directly to the Android system. Any connection to USB devices is through the Lexmark firmware and provided to the Android subsystem to the specific feature that uses the device. For example, firmware updated via a USB device are authenticated by digital signatures; only appropriately authenticated firmware updates are accepted. For more information, see “Protected USB Ports” in the “Secure Access” section of this document.

Rooting

Rooting and Android device is akin to jailbreaking an iPhone; it opens up additional functionality and services to users. The process of gaining root access requires the device to be switched from S-ON to S-OFF (where S means security). Additionally, root is a common exploit used by malicious applications to gain system-level access to your Android. “DroidKungFu” is one such threat that can root a system and install applications at that level; it escapes detection by utilizing encryption and decryption to deliver a payload.

Additionally, Lexmark uses a secure boot as part of the protection. Secure bootloader is used to verify digital signatures on the kernel and each flash partition before it can be mounted by the device. Any changes to Lexmark firmware or to the Android installation would result in a failure to boot the device.

Lexmark Security Measures

The Android subsystem is not running as root directory, but rather in its own chroot that keeps the file system separate from the rest of the device. Running Android in chroot changes the discernable root directory of the file system, thus isolating it from the rest of the firmware. Programs that run in chroot environments cannot access files outside the designated directory structure.

Wi-Fi

Android devices have known vulnerability issues related to unprotected Wi-Fi networks. Some third-party applications can be used to intercept social networking logins of Android devices on their network. Furthermore, Android devices running 2.3 (or rooted older devices) can be used as a Wi-Fi hotspot.

Lexmark Security Measures

Lexmark devices have built-in security measures that require user sign-in credentials which are completed over a secured network. Android communicates with firmware only over local connections and does not accept any remote connections. Additionally, users cannot download third-party applications to the device, and Lexmark devices cannot be rooted.

Security Standards

Common Criteria (NIAP/CCEVS Certification, ISO 15408)

Overview

Common Criteria represents a framework to provide a validation of the security functionality of a computer system. By performing a set of rigorous and repeatable tests, the framework provides participating countries assurance that the product meets the internationally agreed-upon security functional criteria. By meeting the requirements defined in the Common Criteria framework, a product evaluated by one nation is considered to have a valid evaluation by all other nations who have signed the Common Criteria Recognition Arrangement (CCRA). This, in practice, can result in common procurement requirements for the governments that are part of the CCRA.

Benefits

- Third-party validation assures customers that security capabilities protect the device as claimed by the manufacturer.
- Devices are validated using the 2600-2008 IEEE Standard for Information Technology: Hardcopy Device and System Security.
- Two separate validations are performed on Lexmark devices: one with a hard drive and one without a hard drive.

Details

Lexmark devices are validated through a U.S.-based National Information Assurance Partnership (NIAP)–approved laboratory using the latest policy guidance. For the last three evaluation cycles, Lexmark has been validated using the NIAP-approved IEEE 2600 protection profiles, which define the security threats, security functionality to combat those threats and the assurance testing for a class of security devices. The current NIAP-approved protection profile is based on the IEEE 2600.2 or Operational Environment B.

In some cases, Lexmark may have two or more separate evaluations listed with similar model numbers. This is done because some Lexmark devices ship with a hard drive or have other functional differences, which require additional security targets to validate the security capabilities of the device. Adding these other validated devices gives Lexmark customers more options when selecting the appropriate device that meets their internal security requirements.

Federal Information Processing Standards (FIPS)

Overview

FIPS are publicly announced standardizations developed by the United States federal government for use in computer systems by all non-military government agencies and by government contractors. The 140 series of FIPS are U.S. government computer security standards that specify requirements for cryptographic modules.

The FIPS 140 Publication Series is issued by the National Institute of Standards and Technology (NIST) to outline the requirements and standards for cryptographic modules which include both hardware and software components that are used by departments and agencies of the United States federal government. The FIPS 140 standard is an outline of requirements that can be used to provide the necessary conditions to secure information, but should not be, nor is designed to be, a guarantee of information security. The requirements covered within the FIPS 140 publication are documented cryptographic modules and, in some cases, source code around the module.

Benefits

- Third-party validation assures customers that algorithm and/or module meets the requirement as outlined by FIPS.
- Buffered data stored in a device hard drive is secured through a FIPS standard protection mechanism.

Details

Lexmark has also completed a FIPS 140-2 Cryptographic Algorithm Validation Program (CAVP) on the Lexmark devices. This validation provides further assurance of the security of user data while in transit and at rest on Common Criteria–validated devices. CAVP allows for independent validation of the correct implementation of cryptographic algorithms that are used within Lexmark devices.

On current and future devices, Lexmark will not only validate the algorithm used to secure information on the device, but also to validate the cryptographic module through NIST's Cryptographic Module Validation Program (CMVP). CMVP validates the use of cryptographic modules as outlined in FIPS 140-2 for the encryption of all data that has a classification of Sensitive But Unclassified (SBU) or above.

Two Levels of Security

There are two levels of security that are supported based on the product definition. The simplest level of security supports only internal-device authentication and authorization methods. The more advanced level of security permits internal as well as external authentication and authorization, as well as additional restriction capabilities for management, function and solution access. Advanced security is supported for those devices that permit the installation of additional solutions (applications) to the device. In general, if the device supports a touch-screen display, then the security level for that device is advanced.

Simple security utilizes a single PIN to restrict user access to the device's control panel and a single Web page password to restrict administrator access to the device. PIN access for the control panel is specified because text entry is generally difficult on the control panels for these devices while Web page access supports passwords because there are no device panel restrictions. Devices that support simple security are generally used in environments where security risk is limited and advanced security is not required.

Advanced-level security devices support a wide range of local and network authentication and authorization methods. Multiple local authentication functions that support PINs, passwords and username-password combinations for many locally defined users are supported. Standard network authentication through LDAP, LDAP+GSSAPI, Kerberos and Active Directory are supported. Authorization can be specified individually or by groups (either local or network). Devices that support advanced-level security are capable of running installed solutions, which permit the usage of card readers to provide advanced two-factor authentication.

Lexmark

Visit www.lexmark.com for more information.