Security Recommendations for Multifunction Printers

Will Urbanski, ***Virginia Tech IT Security Office and Lab***

September, 2010

Overview

With the rise of the multifunction printer manufacturers were forced to add increased storage capacity in order to meet the storage requirements of the modern office. Internal printer drives contain the documents, scans, and faxes that are sent and received by the printer. Often these documents can remain on the device long after the initial job occurred unless certain security precautions are followed. Because sensitive data is often printed and transmitted electronically it is important to ensure that your printer is protected from several types of attacks that specifically target printers.

Printer security features can be divided into three categories, physical security, network security, and surplus security. Physical security applies to features that protect data from physical theft and harm. If a printer is stolen or the internal drive is removed, physical security features prevent your data from being accessed. Network security applies to features that protect the printer electronically, including the use of encryption and network firewalls. Surplus security applies to features that protect data after the printer is retired from use. Ultimately the security features available on the model dictate whether the device can be surplused with its internal hard drive.

The following pages describe security features that most modern printers support, as well as the kind of attacks that target them. Not every major printer manufacturer supports all of these features; you will need to consult your printer's user guide to determine whether your device supports these technologies.

Printer Security Features

Physical Security

Enable Disk Encryption

Many modern multifunction printing devices support full-disk encryption. Full disk encryption will encrypt the entire contents of the hard drive using a secret key. Using disk encryption prevents a malicious attacker from removing the hard drive from the printer and recovering the documents stored on the disk. The Advanced Encryption Standard (AES) is a popular and preferred form of encryption for use in printers. If the printer manufacturer will not specify the type of encryption they are using the data is likely not being encrypted with an acceptable or approved encryption protocol.

Enable Automatic Disk Wiping

Many modern multifunction printers support some form of automatic disk wiping. The printer will automatically delete old documents when using this feature. If this feature is not enabled most printers will retain old documents until they need to be deleted to free up additional disk space. This practice is extremely dangerous if disk encryption is not enabled.

Enable Automatic Log Wiping

Automatic Log Wiping will delete the print logs on a regular interval. This is different than the "Printer Usage" page provided by most printers, which prints statistics about the toner used and number of pages printed. Enabling this feature on the printer will automatically purge the print logs contained on the printer. Print logs contain information about the user who printed the document including the document name, the file type, the date it was printed, the user's name,

and their IP address. This information could be valuable to a malicious attacker who could use it to discern what kind of documents are stored on a machine, and where the machine is located on the network.

Network Security

Require encryption and a password for the web-interface

Many printers now include a web-based interface that allows administrators to view the printer's status, see reports, configure many aspects of the printer, and print documents from the internet. It is extremely important that a strong password is required for the web-interface. Without a password anyone on the internet can connect to the printer and administer it. Additionally, HTTPS (SSL) encryption should be enabled for the web-based interface. Logging into websites without HTTPS permits passwords to be sent in the clear.

Use or enable a Firewall

Many printers now include a network firewall as a part of the printer operating system. It is very important to limit access to the printer to networks that should have the ability to print. By configuring the firewall to only permit printing from the Virginia Tech network, malicious attackers will be unable to send large print jobs (wasting paper and toner) or perform a Denial of Service (DoS) attack on the printer. Should a printer vulnerability be discovered in the future that allows a malicious attacker to access documents stored on the printer over the network, the printer will be less vulnerable.

If your printer does not have an embedded firewall then you can configure an old, pre-surplus desktop as a simple firewall using a firewall distribution like PFSense.

Surplus Strategies

Clear all logs and data

Appropriately clearing all of the logs and data from a printer involves ensuring the internal logs and stored documents are cleared from the device. It is not enough to just clear the logs! If the printer does not support removing the data then you must remove the hard drive and wipe it manually using a software solution like DBAN.

Reset settings

Clearing the security settings involves resetting the web interface and/or console password. This can usually be done by using the “Restore Factory Settings” functionality.

Secure Wipe

Some devices support an operation called secure wipe which performs a low-level reformat of the internal hard drive. This is different than a simple delete and involves overwriting the data multiple times to ensure that it is not recoverable.

Printer Attacks

Physical Attacks

Theft

Theft of an unsecured printer can result in data loss. Documents, faxes, and electronic communication that have passed through the printer could be compromised without proper encryption.

Malicious misconfiguration

A malicious attacker can alter the configuration of a printer by changing the security settings and potentially gaining access to data. By password protecting the web-based administration panel as well as the console panel, unauthorized configuration changes can be prevented.

Network Attacks

Denial of Service

A network-based Denial of Service attack can render the printer unavailable for the duration of the attack. During such an attack you may be unable to print, scan, or fax documents.

Wasted Resources

Leaving a printer open to printing from unknown networks allows malicious external users to submit large print jobs that can waste toner and paper.

0-day attacks

Unknown flaws may exist in network-enabled printers. By using a network-based firewall you can prevent attackers from exploiting recently released or “0-day” vulnerabilities on your printer before it can be patched.

Surplus Attacks

Document Recovery

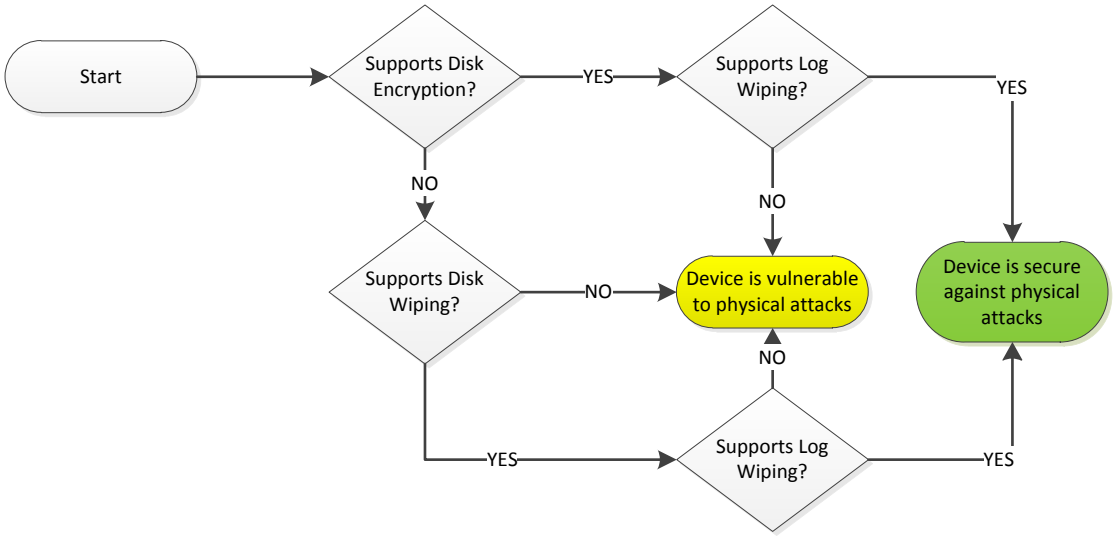
Failure to properly sanitize a printer before it is surplused may allow the next owner to recover sensitive data from it.

Determining your security level

The following sections will allow you to determine whether the printer you are already using or are planning to purchase can be securely operated. You may need to use the printer's user guide or feature information to determine whether or not your printer supports the features mentioned above.

Physical Security

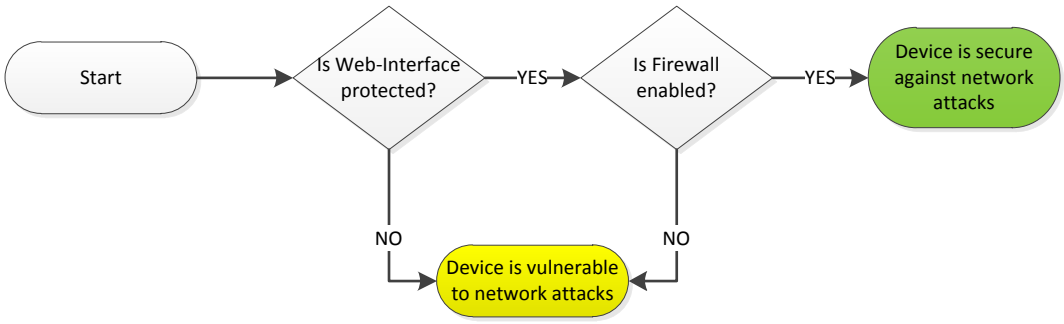
Use the following diagram to determine whether your device is capable of securely storing documents on its internal drive.



Although a physical attack is possible against a device that does not support full disk encryption with automated disk wiping the chances of such an attack being successful are minimal. Even if the data portion of the internal drive is encrypted logs are often stored on a separate printer partition and can still be subject to a physical attack via forensic analysis on the drive.

Network Security

Use the following diagram to determine whether your printer can be secured against network-borne threats.



Surplus Strategies

Use the following diagram to determine whether the internal drive must be removed when the printer is surplused. If Secure Wipe functionality is not supported by the printer then the drive must be removed and reformatted using a NIST-compliant wiping system.