the CENTER for
INTERNET SECURITY

Security Benchmark For

Multi-Function Devices

Version 1.0.0
April 2009

Copyright 2001-2009, The Center for Internet Security

http://cisecurity.org
feedback@cisecurity.org

Terms of Use Agreement

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere (“**Products**”) as a public service to Internet users worldwide. Recommendations contained in the Products (“**Recommendations**”) result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a “quick fix” for anyone’s information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations “as is” and “as available” without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization (“**we**”) agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS’s negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for Multi-Function Devices (MFD)*, provides device agnostic guidance for establishing a secure configuration posture for MFDs. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Background

Over the past decade greater intelligence has been built-in to many enterprise and consumer equipment. Where previously a printer or a fax machine may have been simple to configure via several toggle switches, it may now contain a fully functional operating system and a computer with the processing power dwarfing that of an older desktop computer.

As a result, MFDs have become a prime target for security intrusions. A malicious attacker may compromise the device's operating system, flash storage, and even the multiple network access points to access the corporate network. This is amplified by devices that are never configured beyond what IP address they should use, rarely updated beyond basic asset management, and rarely scanned for vulnerabilities or monitored by an Intrusion Detection System.

The objective of this guide is to help identify and mitigate the security risks that these complex devices introduce to today's network environment.

Consensus Guidance

This guide was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Multi-Function Devices.

Acknowledgements

The following individuals have contributed greatly to the creation of this guide:

Author(s)
Philip Bassil

Contributors and Reviews
Ron Colvin
Glenn Conant

Blake Frantz
Justin Opatrny
Stephen John Smoogen

Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

- be practical and prudent;
- provide a clear security benefit; and
- do not negatively inhibit the utility of the technology beyond acceptable means

Level-II Benchmark settings/actions

Level-II Benchmark recommendations exhibit one or more of the following characteristics:

- may negatively inhibit the utility or performance of the technology
- acts as defense in depth measure

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

Recommendations

1. Physical Device Management

This section provides guidance on the secure configuration of the physical components the Multi-Function Device.

1.1 Physical Connections

1.1.1 Limit Physical Access to Device (Level 1)

Description:
It is recommended that physical access to the MFD be restricted to only authorized users. Additionally, consider segregating print use by data classification or label. For example, it may be inappropriate for personnel from shipping to access a MFD used by the human resources department.

Rationale:
Restricting physical access to the MFD will limit threats against the device's hardware and protect the confidentiality of print, scan, and fax data.

1.1.2 Disable Firewire/1394 Connectors (Level 2)

Description:
Firewire is a physical interface, or connection, commonly used to connect computers, peripherals, and other consumer products. These interfaces are often used by MFDs to provide users with the ability to print documents stored on portable hard drives. It is recommended that Firewire ports be disabled.

Rationale:
Firewire allows a device to have direct memory access (DMA), allowing it to perform I/O without the use of CPU resources. A device connected through a Firewire connection has the potential to write to and read from arbitrary memory locations in the MFD, potentially resulting in reduced levels of data integrity and confidentiality.

References:

- http://www.1394ta.org/Technology/Specifications/specifications.htm

1.1.3 Disable Serial Connectors (Level 1)

Description:
A serial port, such as RS232, is a physical interface, or connection, commonly used to connect computers, peripherals, and other consumer products. These interfaces are often

used by legacy MFDs to provide administrative and diagnostic capabilities. It is recommended that serial connectors be disabled, where possible.

Rationale:
Serial interfaces that expose administrative functionality may be abused by local attackers to compromise the MFD's configuration and the data traversing it.

1.1.4 Require PIN for Administrative Control Panel (Level 1)

Description:
MFDs can commonly be configured to require an authorization code before granting access to the device's control panel. It is recommended that authentication and authorization mechanisms be enabled for administrative control panel access.

Rationale:
Requiring an authentication PIN to administer the MFD will ensure the availability of the device and the integrity and confidentiality of print, fax, and scan data.

1.1.5 Verify Configuration State after Power Loss (Level 1)

Description:
A defective Multi-Function Device may not retain its configuration state after power loss. It is recommended that the configuration state of the MDF be verified after power loss.

Rationale:
If the configuration state of the MFD is not preserved in the absence of power, the device may be exposed to vulnerabilities manifest by its default configuration.

1.2 Hard Drive and Memory Protection

This section provides guidance on securing hard disks and memory of a Multi-Function Device.

1.2.1 Configure Hard Drive Encryption (Level 1)

Description:
MFDs often support the ability to encrypt print jobs while at rest on internal hard drives.

Rationale:
Enabling drive encryption will help ensure the confidentiality of sensitive data in the event a hard disk is stolen or discarded in an insecure manner.

1.2.2 Utilize Chassis or Drive Lock (Level 1)

Description:
MFDs often come equipped with physical locks used to secure internal components.

Rationale:

Utilizing a chassis or drive lock will aid in preventing the theft of internal components such as hard disks and memory. This will in turn protect the confidentiality and availability of print, fax, and scan data.

1.2.3 Delete Completed Scan Jobs (Level 1)

Description:
MFDs often have functionality that allows a user to scan an image to the MFD's local hard drive. It is recommended that the MFD be configured to delete job artifacts once retrieved by the user.

Rationale:
Ensuring that scanned images are deleted from the MFD will help ensure the confidentiality of sensitive data in the event a hard disk is stolen or discarded in an insecure manner.

1.2.4 Erase Hard Drive before Disposal or Return (Level 1)

Description:
MFDs often come equipped with an internal hard disk drive. By default, most manufacturers implement an image overwrite mechanism (also known as Immediate Image Overwrite) that overwrites temporary image files created during the print, network scan, scan-to-email, copy, and fax processes. Once the job has completed, the files are automatically overwritten. Typically, the system administrator can manually invoke this feature using the On Demand Image Overwrite (ODIO) function. Once invoked, ODIO cancels all copy, print, network scan, scan-to-email, and fax jobs, halts the printer interface, and overwrites the portions of the disk used for temporary data storage. It is recommended that this facility be used prior to returning, recycling, or otherwise disposing of the device.

Rationale:
Ensuring that temporary files are overwritten will help ensure the confidentiality of sensitive data in the event a hard disk is stolen or discarded in an insecure manner.

1.3 Firmware

This section provides guidance on the secure configuration of the Multi-Function Device Firmware.

1.3.1 Establish Firmware Currency (Level 1)

Description:
The MFD's operating logic that controls device functionality and service operation is often stored in firmware or Non-Volatile Random Access Memory (NVRAM). It is recommended that firmware revisions remain current.

Rationale:
Ensuring firmware currency will eliminate exposure to published defects and vulnerabilities that have been mitigated in more recent firmware revisions.

2. Remote Device Management

This section provides guidance on the secure configuration of the Remote Device Management features of Multi-Function Devices.

2.1 TCP/IP Configuration

This section provides guidance on the secure configuration of the TCP/IP capabilities of Multi-Function Devices.

2.1.1 Set a Static IP Addresses (Level 1)

Description:
Network devices commonly support two distinct methods for obtaining an IP address; statically and dynamically. Statically assigned IP addresses are typically stored within the device's NVRAM. Dynamically assigned IP addresses are typically obtained at device boot-time via one of many network-based broadcast mechanisms. It is recommended that a static IP address be assigned to the MFD.

Rationale:
The use of static IP addresses reduces the device's exposure to attacks against broadcast IP configuration mechanisms, such as DHCP and BOOTP. Additionally, static IP addresses may increase an organization's ability to effectively monitor and protect the device from network-born threats as the device's IP address will remain constant in Intrusion Detection System (IDS) logs and firewall policies.

2.1.2 Set Static DNS Server Addresses (Level 1)

Description:
The Domain Name System (DNS) is a naming system for networked computers, devices, and resources. It is typically leveraged by network participants to resolve names to and from IP addresses. Network devices commonly support the ability to obtain DNS server addresses via two distinct methods; statically and dynamically. Statically assigned DNS server addresses are typically stored within the device's NVRAM. Dynamically assigned DNS addresses are typically obtained at device boot-time via one of many network-based broadcast mechanisms. It is recommended that DNS server IP addresses be statically configured in the MFD.

Rationale:
The use of static DNS server addresses reduces the device's exposure to attacks against broadcast IP configuration mechanisms, such as DHCP and BOOTP. DHCP and other broadcast mechanisms utilize a UDP transport, which is susceptible to spoofing. If a malicious entity is able to spoof a DHCP response, and therefore control which server the MFD sends DNS requests to, he/she may be able to circumvent security controls on the MFD that leverage name resolution.

2.1.3 Restrict Administrative Access to Specific IP Addresses (Level 1)

Description:

Many MFDs can be configured to limit administrative access to only those connections that originate from a designated IP subnet. It is recommended that access to network accessible administrative interfaces be limited to designated subnets.

Rationale:
Restricting access to the MFD's administrative interface to only a specific set of IP addresses will decrease exposure to unauthorized access. If the device lacks this functionality, use an access control list (ACL) in a router, firewall or switch to restrict access.

2.1.4 Disable Bootstrap Protocols (Level 1)

Description:
Bootstrap Protocols, including BOOTP, PXE, and DHCP are network protocols used by a network client to obtain its network configuration (IP, subnet, DNS servers, gateway, etc) automatically. It is recommended that bootstrap protocols be disabled.

Rationale:
It has been previously recommended that MFD network configuration parameters be assigned statically. This configuration eliminates the need for the MFD to participate in the network bootstrapping process.

2.1.5 Disable Unused Protocols (Level 1)

Description:
Many MFDs can participate in networks that operate over a variety of protocols, including IP, IPX/SPX, and AppleTalk. As a defense in depth measure, it is recommended that all unused network-layer protocols supported by the MFD be disabled.

Rationale:
This configuration will reduce risk introduced by vulnerabilities that are exposed over such protocols.

2.1.6 Disable Universal Plug and Play - UPnP (Level 1)

Description:
UPnP is designed to create a distributed plug-and-play environment over an IP network for the purpose of automatic device discovery, notification, and configuration. It is recommended that UPnP capabilities be disabled to reduce risk introduced by vulnerabilities that are exposed via this mechanism.

Rationale:
If the UPnP capabilities of the MFD are mis-configured, a malicious entity may alter the MFD's configuration which may lead to loss of data integrity, confidentiality, and/or availability.

References:

- http://www.upnp.org/standardizeddcps/security.asp

2.1.7 Confirm Network Ports are Closed (Level 1)

Description:
Research has demonstrated that some MFDs suffer from a mismatch between the service state articulated in the management console and the true state of the service. Given this, it is recommended that the MFD undergo a port scan to ensure only expected network services are available.

Rationale:
Performing a port scan on the MFD will validate that only expected network services are exposed. Additionally, results of the port scan will provide additional security assurance that the device is operating as expected or identify exposures that require additional attention.

2.1.8 Limit Network Accessibility (Level 1)

Description:
Network devices, such as routers and firewalls can be configured to limit ingress traffic to the MFD. It is recommended that network traffic destined to the MFD be limited to authorized subnets and ports.

Rationale:
Limiting the network accessibility of the MFD to only authorized subnets and ports will reduce the exposure of remotely accessible vulnerabilities affecting the MFD.

2.1.9 Restrict Print Services Ports (Level 1)

Description:
Print services are commonly bound to port 9100/TCP or 515/TCP. It is recommended that the MFD be configured to utilize these ports or a port standardized on by the implementing organization.

Rationale:
Configuring the MFD to use a print service port that is known will help ensure the device is visible to network protection and monitoring solutions, such as intrusion detection systems and firewalls.

2.2 Wireless Access Configuration

This section provides guidance on the secure configuration of the Wireless Access capabilities of Multi-Function Devices.

2.2.1 Disable Unused Bluetooth Interfaces (Level 2)

Description:
MFDs often provide administrators and users the ability to interact with the device via Bluetooth, a common short-range wireless communication protocol. Bluetooth allows a user to print and copy from their phone, PDA, or laptop. As a defense in depth measure, it is recommended that unused instances of this interface be disabled.

Rationale:
Disabling Bluetooth interfaces will decrease exposure to latent vulnerabilities in the MFDs Bluetooth protocol parsing stack.

References:

- http://grouper.ieee.org/groups/1451/5/Comparison%20of%20PHY/Bluetooth_24Security_Paper.pdf

2.2.2 Disable Unused Wi-Fi Interfaces (Level 1)

Description:
MFDs often come equipped with Wi-Fi cards that allow these devices to participate on wireless LANs. As a defense in depth measure, it is recommended that unused Wi-Fi interfaces be disabled.

Rationale:
This configuration will reduce risk introduced by vulnerabilities that are exposed over such interfaces. This configuration will also decrease exposure to flaws in the MFDs Wi-Fi protocol stacks.

References:

- http://standards.ieee.org/getieee802/802.11.html

2.3 Use Only Secure Management Protocols

This section articulates the common MFD management protocols that operate over an unencrypted transport. The use of these protocols may create exposures to threats against the integrity of the MFD's configuration, the confidentiality of authentication credentials used by the administrator, and the confidentiality, integrity, and availability of data traversing the MFD.

2.3.1 Disable RSH Access (Level 1)

Description:
RSH (remote shell) is a remote access service utilized by legacy MFDs. It is recommended that this access mechanism be disabled.

Rationale:
The use of this protocol may create exposures to threats against the integrity of the MFD's configuration, the confidentiality of authentication credentials used by the administrator, and the confidentiality, integrity, and availability of data traversing the MFD. Given this, it is recommended that RSH services be disabled. The use of Secure Shell (SSH) is recommended in place of RSH. SSH mitigates the confidentiality and integrity threats that affect RSH.

References:

- http://docs.sun.com/app/docs/doc/816-0211/6m6nc66sv?a=view
- http://www.ietf.org/rfc/rfc4251.txt

2.3.2 Disable FTP Access (Level 1)

Description:
File Transfer Protocol (FTP) is a protocol designed to transfer files between networked devices. Often, MFDs allow users to upload print jobs and print files. Some MFDs also provide the ability to upload files (e.g. scanned documents) to a file server. It is recommended that this access mechanism be disabled.

Rationale:
The use of this protocol may create exposures to threats against the integrity of the MFD's configuration, the confidentiality of authentication credentials used by the administrator, and the confidentiality, integrity, and availability of data traversing the MFD. Given this, it is recommended that FTP services be disabled. The use of FTP over SSH (SFTP) or FTP over TLS/SSL (FTPS) is recommended in place of FTP. SFTP and FTPS mitigate the confidentiality and integrity threats that affect FTP.

References:

- http://www.ietf.org/rfc/rfc959.txt
- http://www.ietf.org/rfc/rfc2228.txt

2.3.3 Disable Telnet Access (Level 1)

Description:
Telnet is a protocol designed to provide interactive text based shell access between networked devices. Legacy MFDs provide administrative access over this protocol. It is recommended that this access mechanism be disabled.

Rationale:
The use of this protocol may create exposures to threats against the integrity of the MFD's configuration, the confidentiality of authentication credentials used by the administrator, and the confidentiality, integrity, and availability of data traversing the MFD. Given this, it is recommended that Telnet services be disabled. The use of Secure Shell (SSH) is recommended in place of Telnet. SSH mitigates the confidentiality and integrity threats that affect Telnet.

References:

- http://www.ietf.org/rfc/rfc854.txt
- http://www.ietf.org/rfc/rfc4251.txt

2.3.4 Secure SNMP Facilities (Level 1)

Description:
SNMP is a network management protocol used for centralized monitoring and configuration of network-based devices. SNMP "traps" are sent to a management console whenever an event occurs that warrants it (e.g. an "out-of-paper" or "paper jam" condition).

The most basic form of SNMP security is the community string, which functions similarly to a password. Many devices come with preconfigured SNMP community strings which pose a security risk if left at the widely known, default settings - "public" for read-only access and "private" for read-write access.

If SNMP is NOT used for device management in your environment, then disable it. If SNMP is used to monitor and/or manage the device, the following recommendations provide increasing levels of protection to better secure SNMP:

1. If only monitoring is necessary, disable SNMP read-write access.
2. Change the default SNMP community strings.
3. If supported by the device and management platform, use SNMPv3.
4. Configure an ACL (on the device and/or network) to limit SNMP queries from only necessary monitoring systems.

Rationale:
By disabling SNMP read-write access and changing the default community string values, the exposure of a malicious entity abusing these facilities to alter the device's configuration is reduced. Additionally, by employing SNMPv3 and ACLs, the device will realize the security benefits of enhanced authentication, confidentiality, and access control capabilities.

References:

- http://www.ietf.org/rfc/rfc1157.txt
- http://www.ietf.org/rfc/rfc2571.txt

2.3.5 Disable Unused SMTP Services (Level 1)

Description:
Simple Mail Transport Protocol, (SMTP) is a protocol designed to transfer mail reliably and efficiently. Some MFDs accept inbound SMTP requests in support of SMTP-to-fax services. It is recommended that this access mechanism be disabled if unused.

Rationale:
The use of this protocol may create exposures to threats against the confidentiality and integrity of print jobs. Given this, it is recommended that SMTP services be disabled. Additionally, it may be possible for a malicious entity to abuse MFD SMTP services for nefarious purposes, such as sending unsolicited email. SMTP over TLS/SSL will mitigate passive and casual attacks against the confidentiality and integrity of print jobs while in transit over SMTP. The use of SMTP over TLS is recommended in place of SMTP as it mitigates the confidentiality and integrity threats that affect SMTP.

References:

- http://www.ietf.org/rfc/rfc0821.txt
- http://www.ietf.org/rfc/rfc2487.txt

2.3.6 Disable Unused HTTP Services (Level 1)

Description:
Hyper Text Transfer Protocol (HTTP) is the primary protocol over which web based communications occurs. Often, MFDs utilize this protocol to expose rich administrative interfaces. It is recommended that this access mechanism be disabled in favor of HTTPS.

Rationale:
The use of this protocol may create exposures to threats against the integrity of the MFD's configuration, the confidentiality of authentication credentials used by the administrator, and the confidentiality, integrity, and availability of data traversing the MFD. Given this, it is recommended that HTTP services be disabled. The use of HTTP over TLS/SSL (HTTPS) is recommended in place of HTTP as HTTPS mitigates the confidentiality and integrity threats that affect HTTP.

References:

- http://www.ietf.org/rfc/rfc2616.txt
- http://www.ietf.org/rfc/rfc2818.txt

3. Job Access and Processing

This section provides guidance on the secure configuration of the Multi-Function Device with respect to print job access Processing.

3.1 Authorized Job Retrieval and Submission

3.1.1 Require PIN for Confidential Job Retrieval (Level 1)

Description:
Many MFDs can be configured to require a pin or RFID interaction to retrieve print jobs. It is recommended that a PIN, or other authorization mechanism, be required to access print jobs.

Rationale:
Leveraging a job retrieval authorization mechanism, such as a PIN, will ensure the confidentiality of print, fax, and scan jobs.

3.1.2 Accept Jobs from Only Authorized Spoolers and Users (Level 1)

Description:

It is recommended that print jobs be restricted to only those jobs that originate from authorized spoolers or users.

Rationale:
By limiting access to device print services to only authorized spoolers and users the exposure to load-based denial of service attacks is reduced.

4. Application Development Platforms

This section provides guidance on the secure configuration of the Multi-Function Device with respect to its application development platform.

4.1 Application Signatures

4.1.1 Require Valid and Trusted Signature for all Applications (Level 1)

Description:
Many enterprise class MFDs have development platforms that allow corporations to load software packages onto the device. These packages are typically designed to alter user interfaces, perform pre or post job processing such as encryption, or perform network operations. MFDs having this capability may support a configuration that requires all packages contain a valid digital signature of a trusted application developer.

Rationale:
Ensuring the integrity and authenticity of applications and software packages installed on the MFD will ensure print job confidentiality, integrity, and availability. Configuring the MFD to require all packages and application contain a valid digital signature of a trusted developer will assist in this assurance.

References:

- http://www.rsa.com/rsalabs/node.asp?id=2182

4.1.2 Require Application Certificate be signed by a Trusted Authority (Level 1)

Description:
Many enterprise class MFDs allow corporations to load software packages onto the device. These packages are typically designed alter user interfaces, perform pre or post job processing such as encryption, or perform network operations. MFDs having this capability may support a configuration that requires all packages contain a certificate that has been signed by a trusted certificate authority (CA), or root.

Rationale:
Ensuring that all application certificates are signed by a trusted root will ensure the authenticity of the application's signature. This will in turn provide additional assurance that the integrity of the application being loaded on to the MFD is intact.

References:

- http://www.rsa.com/rsalabs/node.asp?id=2278

4.2 Package Management

4.2.1 Uninstall or Disable all Unused Packages (Level 1)

Description:

Multi-Function Devices often come equipped with software-based features that may not be utilized. It is recommended that unused software-based features be disabled.

Rationale:
Uninstalling or disabling utilizing software packages will reduce the attack surface of the Multi-Function Device.

5. User Management

This section provides guidance on the secure configuration of the user and account management capabilities of the Multi-Function Device.

5.1 Default Accounts

5.1.1 Change Default Passwords (Level 1)

Description:
Multi-Function Devices are typically configured with default user accounts that are common to all devices of the same make/model. It is recommended that default passwords be changed.

Rationale:
Changing the default password for all default accounts will reduce the probability of unauthorized access to the device.

5.1.2 Rename Default Accounts (Level 1)

Description:
Multi-Function Devices are typically configured with default user accounts that are common to all devices of the same make/model. It is recommended that default usernames be changed.

Rationale:
Renaming default accounts will reduce an attacker's ability to ascertain valid device credentials.

6. Logging and Monitoring

This section provides guidance on the secure configuration of the logging and monitoring capabilities of the Multi-Function Device.

6.1 Enable Logging

6.1.1 Enable Print Spooler Access Logging (Level 1)

Description:

Print spoolers typically contain functionality to log all submitted requests. It is recommended that these facilities be enabled on the print spooler, logging levels be set to ensure adequate details are preserved, and logs be reviewed.

Rationale:
When a security event occurs, spooler access logs may provide investigators with information necessary to determine the extent and origin of the event.

6.1.2 Enable Print Job Logging (Level 1)

Description:
MFDs commonly contain functionality to log all submitted requests. It is recommended that these facilities be enabled on the device, logging levels be set to ensure adequate details are preserved, and logs be reviewed.

Rationale:
When a security event occurs, these logs may provide investigators with information necessary to determine the extent and origin of the event.

6.1.3 Enable Print to Fax Logging (Level 1)

Description:
Multi-Function Devices that contain print to fax capabilities typically contain functionality to log all such requests including the destination fax number. It is recommended that these facilities be enabled on the device, logging levels be set to ensure adequate details are preserved, and logs be reviewed.

Rationale:
When a security event occurs, these logs may provide investigators with information necessary to determine the extent and origin of the event. Additionally, these logs may be useful to isolate information leaks.

6.1.4 Enable Print to Email Logging (Level 1)

Description:
Multi-Function Devices that contain print to email capabilities typically contain functionality to log all such requests including the destination email address. It is recommended that these facilities be enabled on the device, logging levels be set to ensure adequate details are preserved, and logs be reviewed.

Rationale:
When a security event occurs, these logs may provide investigators with information necessary to determine the extent and origin of the event. Additionally, these logs may be useful to isolate information leaks.

6.1.5 Enable Print to Share Logging (Level 1)

Description:

Multi-Function Devices that contain print to file share capabilities typically contain functionality to log all such requests including the destination email address. It is recommended that these facilities be enabled on the device, logging levels be set to ensure adequate details are preserved, and logs be reviewed.

Rationale:
When a security event occurs, these logs may provide investigators with information necessary to determine the extent and origin of the event. Additionally, these logs may be useful to isolate information leaks.

7. Miscellaneous Recommendations

This section provides guidance on the secure configuration of miscellaneous capabilities of the Multi-Function Device.

7.1 Certificates

7.1.1 Replace Self-Signed Certificates (Level 1)

Description:
Print devices often utilize self-signed certificates to protect the communication between administrators and management interfaces. This is most commonly found when managing the device via an HTTPS interface. It is recommended that self-signed certificates be replaced by certificates that chain to a trusted certificate authority.

Rationale:
Self-signed certificates are less effective at ensuring that the communication between the administrator and the management interface is not victim to a man in the middle attack. This is because the identity of the certificate holder is not attested to by a trusted third party. Given this, it is more feasible for a malicious entity to compromise administrative communication by generating his/her own self-signed certificate and presenting that certificate to the administrator's HTTPS client on behalf of the MFD.

7.2 File Shares

7.2.1 Secure Scan to Share Locations (Level 1)

Description:
Multi-Function Devices often support placing scans on a remote file share. It is recommended that access to these file shares be restricted.

Rationale:
Limiting access to these file shares will help protect the confidentiality of scanned data by reducing the probability of an unauthorized individual accessing that data while it is stored on the file share.

Appendix A: References

1. Defense Information Systems Agency (2009). *Multi-Function Device (MFD) and Printer Checklist for Sharing Peripherals Across the Network.* Available: http://iase.disa.mil/stigs/checklist/span_mfd_checklist_v1r1-3_04_15_2009.pdf. Last accessed 22 April 2009.

2. Hewlett Packard (2009). *Secure imaging and printing.* Available: http://h71028.www7.hp.com/enterprise/cache/617605-0-0-225-121.html. Last accessed: 10 April 2009

3. PC World (2005). *Multi-Function Devices.* Available: http://www.pcworld.idg.com.au/article/173242/multi-function_devices. Last accessed 10 April 2009.

4. eWeek (2008) *Multifunction Printers: The Forgotten Security Risk.* Available: http://www.pcworld.idg.com.au/article/173242/multi-function_devices. Last accessed 10 April 2009.

5. Xerox (2004). *Image Overwrite Security for the Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System Security Target.* Available:http://www.dsd.gov.au/library/pdfdocs/EPL_Listings_ST_CRs/miscellaneous_pdf/Xerox/imageoverwriteST.pdf. Last accessed 10 April 2009.

6. University of Texas (2009). *Multifunction Printer Hardening Checklist.* Available: http://security.utexas.edu/admin/mfprinter.html. Last accessed 10 April 2009.

7. Hewlett Packard (2006). *HP LaserJet 4345 MFP Security Checklist.* Available: http://www.hp.com/united-states/business/catalog/nist_checklist.pdf. Last accessed: 10 April 2009.

8. RSA (2009). *Crypto FAQ.* Available: http://www.rsa.com/rsalabs/node.asp?id=2182. Last accessed: 10 April 2009.

9. RSA (2009). *Crypto FAQ.* Available: http://www.rsa.com/rsalabs/node.asp?id=2278. Last accessed: 10 April 2009.

10. 1394 Trade Association (2009). *Specifications.* Available: http://www.1394ta.org/Technology/Specifications/specifications.htm. Last accessed: 10 April 2009.

11. UPnP Forum (2003). Device *Security and Security Console V 1.0.* Available: http://www.upnp.org/standardizeddcps/security.asp. Last accessed: 10 April 2009.

12. IEEE Bluetooth SIG Security Expert Group (2002). *Bluetooth™ Security White Paper.* Available: http://grouper.ieee.org/groups/1451/5/Comparison%20of%20PHY/Bluetooth_24Security_Paper.pdf. Last accessed: 10 April 2009.

13. IEEE Standards Association (2008). *IEEE 802.11 LAN/MAN Wireless LANS.* Available: http://standards.ieee.org/getieee802/802.11.html. Last accessed: 10 April 2009.

14. IETF (2006). *The Secure Shell (SSH) Protocol Architecture.* Available: http://www.ietf.org/rfc/rfc4251.txt. Last accessed: 10 April 2009.

15. IETF (1985). *FILE TRANSFER PROTOCOL (FTP).* Available: http://www.ietf.org/rfc/rfc959.txt. Last accessed: 10 April 2009.

16. IETF (1997). *FTP Security Extensions.* Available: http://www.ietf.org/rfc/rfc2228.txt. Last accessed: 10 April 2009.

17. IETF (1983). TELNET PROTOCOL SPECIFICATION*.* Available: http://www.ietf.org/rfc/rfc854.txt. Last accessed: 10 April 2009.

18. IETF (1990). *A Simple Network Management Protocol (SNMP).* Available: http://www.ietf.org/rfc/rfc1157.txt. Last accessed: 10 April 2009.

19. IETF (1999). *An Architecture for Describing SNMP Management Frameworks.* Available: http://www.ietf.org/rfc/rfc2571.txt. Last accessed: 10 April 2009.

20. IETF (1982). *SIMPLE MAIL TRANSFER PROTOCOL.* Available: http://www.ietf.org/rfc/rfc0821.txt. Last accessed: 10 April 2009.

21. IETF (1999). *SMTP Service Extension for Secure SMTP over TLS.* Available: http://www.ietf.org/rfc/rfc2487.txt. Last accessed: 10 April 2009.

22. IETF (1999). *Hypertext Transfer Protocol -- HTTP/1.1.* Available: http://www.ietf.org/rfc/rfc2616.txt. Last accessed: 10 April 2009.

23. IETF (2000). *HTTP Over TLS.* Available: http://www.ietf.org/rfc/rfc2818.txt. Last accessed: 10 April 2009.

24. Sun Microsystems (2001). *man pages section 1M: System Administration Commands.* Available: http://docs.sun.com/app/docs/doc/816-0211/6m6nc66sv?a=view. Last accessed: 10 April 2009.

Appendix A: Change History

Date	Version	Changes for this version
April 25, 2009	1.0.0	Initial Public Release

Appendix B: CIS/DISA SPAN STIG Mapping

These mappings are provided to assist those adopting the CIS Benchmark and SPAN STIG.

Benchmark Item	STIG Item(s)
1.1.1	NA
1.1.2	NA
1.1.3	NA
1.1.4	MFD08.002
1.1.5	MFD02.002
1.2.1	NA
1.2.2	MFD08.001
1.2.3	MFD07.002
1.2.4	MFD06.002
1.3.1	MFD02.004
2.1.1	MFD01.002
2.1.2	NA
2.1.3	MFD02.005
2.1.4	MFD02.003
2.1.5	MFD01.001
2.1.6	NA
2.1.7	NA
2.1.8	MFD01.003
2.1.9	MFD03.001
2.2.1	NA
2.2.2	NA
2.3.1	MFD02.003
2.3.2	MFD02.003
2.3.3	MFD02.003
2.3.4	MFD02.003
2.3.5	MFD02.003
2.3.6	MFD02.003
3.1.1	NA
3.1.2	MFD06.001, MFD05.001
4.1.1	NA
4.1.2	NA
4.2.1	NA
5.1.1	NA
5.1.2	NA
6.1.1	MFD06.001
6.1.2	MFD06.001
6.1.3	MFD07.004
6.1.4	MFD06.001
7.1.1	NA
7.2.1	MFD07.003

STIG Item	Benchmark Item(s)
MFD01.001	2.1.5
MFD01.002	2.1.1
MFD01.003	2.1.8
MFD02.001	2.3.4
MFD02.002	1.1.5
MFD02.003	2.3.1 - 2.3.6, 2.3.4
MFD02.004	1.3.1
MFD02.005	2.1.3
MFD03.001	2.1.9
MFD04.001	3.1.2
MFD05.001	3.1.2
MFD06.001	6.1.1, 6.1.2
MFD06.002	NA
MFD06.006	6.1.1 - 6.1.5
MFD07.001	NA
MFD07.002	1.2.3
MFD07.003	7.2.1
MFD07.004	6.1.2
MFD07.005	2.3.4
MFD08.001	1.2.2
MFD08.002	1.1.4