Security Threats and Measures on Multifunctional Devices

J. Botha[1], S. Von Solms[2]
[1]Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
[2]Department of Electrical Engineering, Faculty of Engineering and the Built Environment University of Johannesburg, Johannesburg, South Africa

[1]jbotha1@csir.co.za
[2]svonsolms@uj.ac.za

Abstract: Multifunctional devices are employed in office networks for functionality and comfort, most often considered only as peripheral devices enabling the printing, copying and scanning of documents. Based on a study performed by InfoTrends in 2013 in the USA and Western Europe, the majority of people surveyed are of the opinion that computers pose the biggest security threats of all technological devices (Forbes, 2017a). In many cases, users of multifunctional devices do not realise that a multifunctional device is also a network device which have similar vulnerabilities, whereby the security threats relating to these devices are often overlooked. This paper provides an overview of the physical and network security risks relating to networked multifunctional devices. It includes a number of experiments and tests performed on multifunctional devices, security analysis, discussions on possible exploits as well as recommendations on various security measures. This paper could serve as a high-level guideline when installing multifunctional devices in a network environment and informing administrators and users of the security risks associated with installation and daily use.

Keywords: data extraction, multifunctional device, networks, printers, risk, security

1. Introduction

More or less all multifunctional devices (MFDs), or multifunctional printers (MFPs), built after 2002 contain a hard drive (Forbes.com, 2017a; Kassner, 2010), not only offering printing capabilities, but a range of additional capabilities such as copying and scanning. These devices can be assigned Transmission Control Protocol/Internet Protocol (TCP/IP) addresses and can act as standalone units accessible online. To host these capabilities, MFDs have their own embedded operating systems as well as TCP/IP ports (Baker, 2012; Condon et al, 2011). Network devices offer additional capabilities, which include the sharing of printers by multiple users. In addition, storage facilities may be present where printed, scanned or copied data is stored onto the hard drive (Condon, Cummins, Cukier & Afoulki, 2011; Kassner, 2010). Usually, when several copies of a document are needed, the document is scanned once and copies are made of the file saved on the hard disk of the device.

These features are very useful in an office environment, but can pose major security threats if not protected. In general, the security risks on networked MFDs can be divided into four areas: unclaimed output; unauthorised access to print, scan, email and copy functions and device configurations; latent images on the hard disk/removable drive and network security risks (Capital Document Solutions, 2017). This paper considers these vulnerabilities on network printers used in offices today.

This paper is structured as follows: Section two describes the tools that can be used to find vulnerable printers on a local network and on the Internet. Sections three include discussions on physical and networking security risks. Section four contains an overview on experiments performed using certain tools and methods, attempting to exploit MFDs. Section six includes the security measures and recommendations. The paper concludes with section six.

2. Exploration of Devices

When a MFD is connected to an office network and not fully secured, the devices can be left vulnerable to outside attackers. Like a computer added to a network without any firewalls, passwords and anti-virus tools to protect it, these devices are open to exploitation. Every MFD with enabled network services has a web interface, which enables users to use the provided services over the network via the interface. If a network printer is unprotected, an attacker can access its web interface over the Internet.

Several tools, freely available on the Internet, allows an attacker to search for printing devices accessible through a local network and the Internet. Tools such as Soft Perfect Network Scanner[1], NMAP[2] (the Network Mapper - Free Security Scanner) or Cain & Abel[3] can be used to find printers on a local network. Finding printer devices on the Internet can also be done by entering specific search strings into Google[4]. Table 1 shows the search strings that can be used to find unprotected printers over the Internet by means of a Google search (Crenshaw, 2017).

Table 1. Search strings to find unprotected printers through a Google search

Search String	Results
Inurl: HP/device/this. LCDispatcher	HP JetDirect printers.
inurl:"/en/sts_index.cgi"	Ricoh Savin printers.
intitle:"web image monitor"	Ricoh Savins using web monitors.
/web/user/en/websys/webArch/mainFrame.cgi	Ricoh Savin printers.
inurl:":631/printers" -php -demo	Common UNIX printing system(CUPS) (Ward, 2005) connected to printers.

Figure 1 shows some of the results using the HP JetDirect search string in search for printers over the Internet using Google.

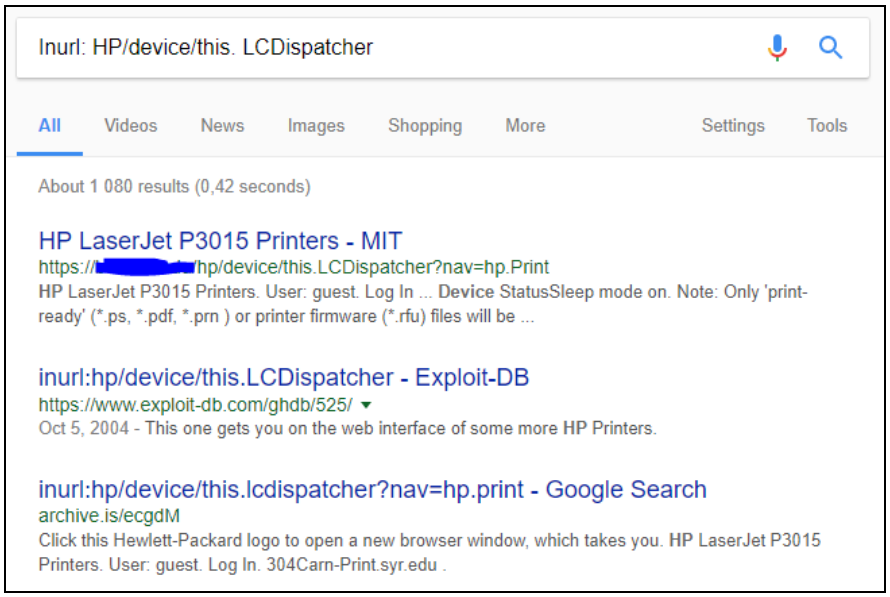

Figure 1. HP JetDirect Printers – Google Search Results

A more detailed search on the Internet for devices can be conducted through the use of Shodan[5], a website that searches for unprotected devices connected to the Internet (see Figure 2). Shodan allows for more specific searches, for example: to only search for HP printers in South Africa. Not only does the search results provide the attacker with the Internet Protocol (IP) addresses of the devices, but also include information regarding the software installed on the device as well as location details and links to the web interface. In addition, Shodan allows the export of results into a downloadable file. The saved search results can be used as input in custom written programs to exploit multiple devices.

[1] www.softperfect.com
[2] www.nmap.org
[3] www. oxid.it
[4] www.google.co.za
[5] www.shodan.io

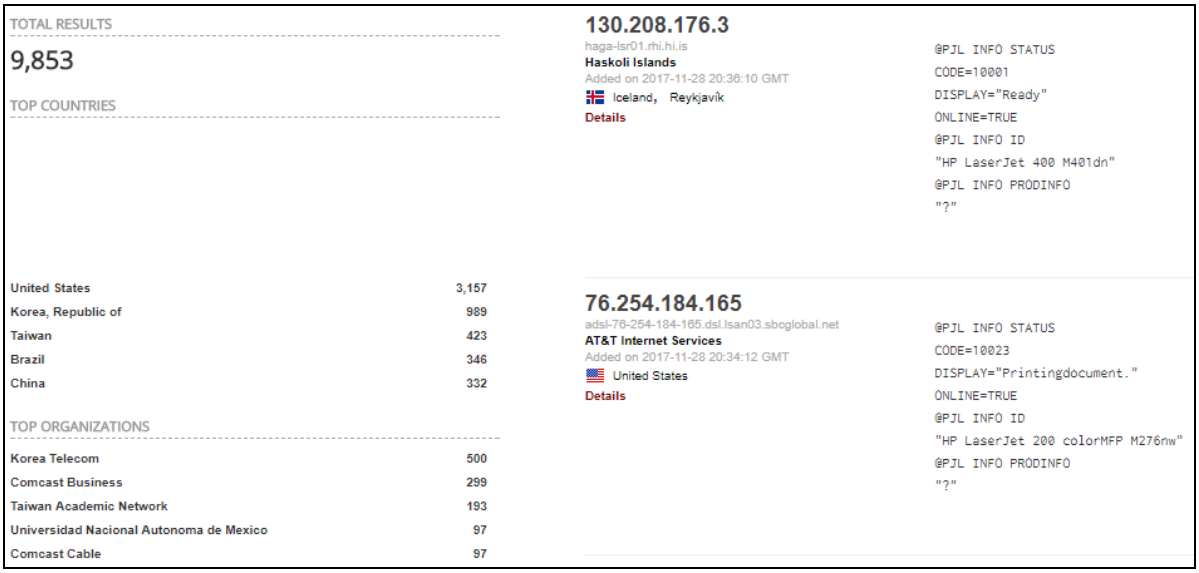

Figure 2. HP Shodan Search Results

From the above examples it can be seen that if printers are not protected, a complete detailed view of the printer configurations can be obtained through simple online searches or tools. Without password authentication, or with the default password enabled, these devices can be controlled remotely through the use of the printer's web interface (Stover, 2004). With administrator access, it is possible to change configuration settings, change the administrator password and even perform firmware updates.

3. Security Risks

This section discusses some of the security risks involved with MFDs.

3.1 Physical Access to a Printer

When printing, some MFDs store the printed documents onto the hard disk drives (HDDs) of the printer (TechRepublic, 2017). The risk is that the HDDs of many MFDs can be removed from the device. Deleted files that are not yet overwritten could be "undeleted" by connecting the hard drive to a PC and using recovery utilities such as Recuva (Piriform.com, 2017).

A person without the required authorisation can physically capture print jobs and scanned documents that are unclaimed at the device. In addition, MFDs with email functionalities are vulnerable to the capture of email addresses and fax numbers. When the MFD's administrator password is disabled or not changed from the default, an unauthorised person can gain access to the settings of the device and make changes. Several MFDs have manual administrator password overwrite functions where the administrator password can be reset without requiring the administrator password.

3.2 Network

3.2.1 Web Portal

Most MFDs have embedded web servers and management consoles that can be accessed through several network protocols (Support.hp.com, 2017a). If these protocols are not securely set-up, it may pose network security risks (University of Hawaii, 2017). Another risk is, by default, the web interfaces of MFDs usually do not need a password for access or it is set up with a default administrator password (Support.hp.com, 2017a).

Some printer's web servers are vulnerable to cross-site scripting exploits. Cross-site scripting is found in web applications when an attacker injects malicious client-side scripts into the web pages (Acunetix, 2017). These exploits are able to trick a user into believing they are connecting to, for example, a printer's web server, when they are actually communicating with a hacker (Kirda, Kruegel, Vigna & Jovanovic, 2006, SANS Internet Storm Centre, 2017). When being a victim of this type of attack, the attacker could steal a user's session cookie and be able to impersonate the victim. A cookie is a small piece of data stored on the user's browser, allowing to indicate if different web requests come from the same browser. This is used to keep a user logged into a

specific website. It might also be possible to get the victim's geolocation if it was shared on the infected browser (Acunetix, 2017).

3.2.2 Telnet

Telnet is an unsecure text-based configuration and management interface. Due to the lack of encryption, authentication and configuration information can be easily sniffed (Fei, Jones, Lakkas, & Zheng, 2002). In many MFDs, the Telnet protocol is enabled by default, allowing n an attacker can gain access (Vail, 2003). Telnet can be used to modify the network, modify the printer password, access information about print queues and to monitor printer activity. A hacker could Telnet into a printer and change the printer's IP address, making it vulnerable to Denial of Service (DoS) attacks.

In the Windows 2000 Telnet service, a vulnerability exists due to a handle leak when a Telnet session is terminated. An attacker could keep starting sessions and then terminating them, exhausting the supply of handles on the server to the point where it could no longer perform useful work. This process of starting and terminating sessions would result in a DoS attack (Microsoft, 2017).

Another attack possible with is if the user's computer has Intrusion Prevention Systems (IPS) installed and the user tries printing to a network printer, an error that indicates a DoS attack is received. This happens because some printers communicate over User Datagram Protocol (UDP) using raw mode. If the printer sends too many UDP packets in a certain time period, the UDP Flood Attack is triggered. This is a form of DoS attack as it interrupts the printer's service.

A connection to port 9100/TCP is single threaded (Crenshaw, 2017). When making a connection via Telnet and holding the connection, no other print jobs will be allowed to the printer. The connection should time-out after a while allowing the acceptance of print jobs again.

3.2.3 Simple Network Management Protocol (SNMP)

SNMP is a network protocol used to manage TCP/IP networks(Technet.microsoft.com, 2017). Simple default passwords are used by SNMP and is always active by default. When the password is changed, the default password is still stored in a variable which can be accessed by someone who knows the address of the printer and location of the variable (Vail, 2003). SNMP reveals network structure information and is therefore considered an unsecure protocol. A network scanning tool such as Zenmap[6] can be used to find more information regarding the printer and network configurations when SNMP is active.

3.2.4 File Transfer Protocol (FTP)

FTP provides printers with the ability to upload files to the MFD. Authentication of an FTP session and the transferring of the file over FTP is not encrypted, therefore log-in credentials and data can be sniffed by a potential attacker (Gromek, 2002; Docstore.mik.ua, 2017).

Printers can be vulnerable to a FTP bounce attack, where hackers gather information about a network. A bounce attack is where some printers offer anonymous FTP servers for dropping print jobs. These servers allow passive mode FTP and have a 'get' command which can be used by hackers to use the server as a proxy server to forward packets while hiding their identity, allowing the attacker to be untraceable (Vail, 2003; InfoSec, 2015).

3.2.5 HP JetDirect

The HP Direct protocol uses port 9100 and is one of the most widely used for network printers (Support.hp.com, 2017b). JetDirect passwords are stored in plain text and are easily accessible via SNMP. This means that any unauthorised person with malicious intent can gain access to the password. Through JetDirect, the message on the display panel of a printer can be modified. The ability to modify a printer's display panel could potentially open doors to social engineering.

[6] http://nmap.org/zenmap

3.2.6 Internet Printing Protocol (IPP)

IPP sends print jobs to printers over the network (Tools.ietf.org, 2017). What has been discovered is, if access to a printer is not restricted to authorised users, anyone can access it and perform remote printing. Printing jobs can be intercepted via network sniffing or an unprotected printer can be spammed by sending large print jobs to the printer (Tools.ietf.org, 2017).

3.2.7 Line Printer Remote (LPR) & Line Printer Daemon (LDP)

LPR is a connectivity tool that runs on client computers and that is used to print files to a computer running a LPD server. LPD is a service on a print server that receives print jobs from the LPR tools (Beal, 2017). Jobs that are sent to the printer, using LPR, are sent in clear text and can therefore be sniffed off the network. Due to the lack of security and encryption, unauthorised printing can be done.

A number of security risks exist when using an unprotected MFD on a network. Table 2 shows a summary of the risks posed by the networking protocols discussed above.

Table 2. Network Security Risks

Protocol	Ports	Risks
HTTP	80, 8080	The information is not encrypted and can be viewed easily. Vulnerable to cross-site scripting exploit and DoS attacks
HTTPS	443	The more secure version of HTTP for data is encrypted.
Telnet	23	Unencrypted protocol. Can modify the network; modify printer password; access information about print queues; change printer's IP address. DoS attacks.
SNMP	161, 162	Simple default passwords. Reveals a lot of network information that can be used for attacks.
FTP	21	Unencrypted authentication and transferring of files. Vulnerable to FTP bounce attacks and dropping of print jobs.
JetDirect	9100	Passwords stored in text, therefore exposed to unauthorized printing, capturing of spool files.
IPP	631	Unauthorized remote printing. Print job interceptions; printer Flooding.
LPR	721-731	Jobs sent in clear text, no encryption. Print jobs can be intercepted over the network; unauthorized printing can be done.
LPD	515	Same as for LPR.

3.3 Firmware Update

The firmware of various printers can be uploaded via parallel cable, USB cable or USB device. Reverse engineering on the firmware is possible to change the contents thereof. Older devices do not verify the source of the firmware (Forbes.com, 2017b; Sullivan, 2011) and thus the changed firmware may be accepted and installed by the devices. The firmware could be changed to do activities unknown to the operator such as forwarding copies of printed documents to a remote machine or adding features such as network sniffers (Sullivan, 2011; Vijayan, 2011). When the modified firmware is sent to the printer via the USB port or web interface by an attacker, the security of the MFD is compromised.

4. Experiments: Tools and Methods to Exploit MFDs

This section discusses experiments performed by the researcher on possible ways to exploit unprotected printer devices, using various tools and methods.

4.1 Physical Access to a Printer

With this study, physical access was obtained to a network printer and the HDD was removed. Using a HDD recovery tool, such as Recuva, it was possible to obtain certain files from the printer hard drive. Even when files were deleted, it was possible to recover the deleted files.

With physical access, it is also possible to perform a cold reset on the device. This will overwrite the administrator password to the defaults. With the administrator password changed, all the network and security settings, passwords as well as email addresses on the MFD can be changed by the attacker. The firmware of the MFD can be updated with physical access, but was not done during this study.

4.2 Network

4.2.1 Hijetter

Hijetter[7] is a standalone executable program that enables the user to explore HP printers via the Print Job Language (PJL) interface. PJL is supported by later versions of the Printer Control Language (PCL). Hijetter connects to port 9100 of the printer and enables the user to manipulate the printer via PJL commands. The user must enter the IP address of the printer to make a connection. When connected, Hijetter provides three dialogs that can be selected: The file dialog, the environmental variables dialog and the message display dialog.

Using the the message display dialog, it was possible to set a printer in a failure status. The failure state will prevent any device to print documents to the printer. The printer might still display the message "*Ready*" on the LCD when no message was captured, but when printing documents from any computer or device, it will give an error message stating "*Error-Printing*". The only way to set the printer in a ready status and allow printing again was to physically restart it, thus resulted in a Denial of Service (DoS) attack. A DoS attack is an interruption of service due to the system being destroyed or being unavailable (Mirkovic, Dietrich, Dittrich & Reiher, 2004). DoS attacks can be used to target printers so they are unable to print for a certain period of time. The environmental dialog of Hijetter lists all variables for the printer. These variables or printer properties including username, password, paper size and quantity can be changed. The program sends the corresponding command to the printer via PJL in order to change the printer settings.

The message on the LCD display of a printer could also be changed by using the display dialog option as seen in Figure 3. Figure 4 below shows the LCD screen of an HP P4015 printer after it has been changed via Hijetter.

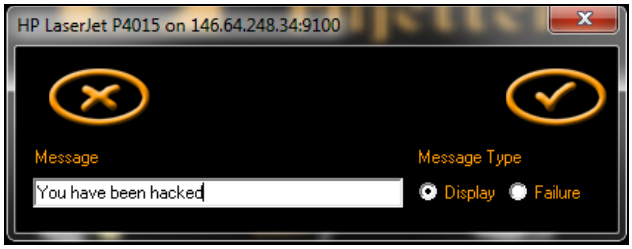

Figure 3. Display Dialog of Hijetter

Figure 4. LCD of HP P4015

The alteration of the ready message can be used as a tool by the attacker for social engineering. For example: ***Error: call 012 345 6789*** where the number can belong to the attacker.

4.2.2 Web Portal

Some of the local HP printers as well as the printers found within the Internet search, had default administrator passwords set or no password at all. When logged into a local HP printer, via the printer's web portal, using the default administrator credentials, it was possible to change the IP address, subnet mask and default gateway of the device. This resulted in a DoS attack, as no one connected to the printer could perform any print jobs. This was not performed on the MFDs found on the Internet due to ethical reasons.

It was also possible to change certain security settings, including the encryption, authorisation and used protocols on the local MFD. The network settings could also be changed, enabling the printer to receive print jobs from remote sites. If the printer is not restricted to authorised users only, anyone can access it and perform remote printing. It was also possible to alter the stored user's email addresses. When using the scan to email functionality, the scanned documents will go to an unintended email address.

[7] http://www.phenoelit.org/hp/

4.2.3 Telnet

If the administrator password is not set, it is possible to access the device to the default password using Telnet. From the command prompt it was possible to gain access to certain local printers, change IP addresses and network configurations. This resulted in a DoS attack as the printers were not accessible through the network. Table 3 contains Telnet commands for changing network configurations (Brother Solutions Center, 2017). The viewing and changing of passwords and enabling/disabling of protocols was also possible (Technet, 2011).

Table 3. Telnet Commands for Printer Network Settings

Action	Command
Connect to host printer	*TELNET IP Port*
Change IP Address	*SET IP ADDRESS 192.168.1.3*
Set subnet mask	*SET IP SUBNET 255.255.255.0*
Set the router address	*SET IP ROUTER 192.168.1.3*
Set IP access config to static	*SET IP METHOD STATIC*
Exit Telnet	*EXIT or Ctrl-D*

4.2.4 IPIterator

IPIterator, a command line tool for Linux, enables an attacker to flood the printer with bulk messages. The tool only works if port 9100 is open (Crenshaw, 2017). All one has to do is to generate a Postscript (Howtogeek.com, 2011) file with some content you want to send to the printer. The message can then be sent to a whole network range. It can also be used to send mass messages to a network. In addition, it enables the user to attach a whole hard drive's content to the print job causing the size of the print job to be too big. Table 4 shows the commands that can be used with IPIterator. These tests were not performed in this study, due to no permission granted to run the tests in the company environment where the research was performed.

Table 4. IPIterator Commands

Action	Command
Flood printer	./ipiterator192.168.3.1-5,25,"spam.prn|netcat -q 0 ~ip 9100"
Attach a whole hard drive to the print job causing the size of the print job to be too big	cat /dev/hda|netcat -q 0 192.168.1.2 9100
Hold a connection to a whole network range, knocking out print jobs on the whole LAN	./ipiterator 192.168.1.*,25,"telnet ~ip 9100"

4.2.5 Postscript

Postscript (PS) is a programming language describing the appearance of a printed page. PS is processed when a user writes a document and prints it. A PS driver converts the print data to a PS stream which is rendered by the printer (Howtogeek.com, 2011). PS can easily be used to attack networks and systems. By adding an infinite loop in the postscript file sent to the printer, some printers will hang, which can serve as a DoS attack. This test was also not performed in this study.

4.2.6 Man in the Middle (MITM)

In order to intercept documents over the network, a man-in-the-middle (MITM) attack can be performed. It is a technique where the attacker's machine will make independent connections between the target and the host machine. In this case the printer acts as the host, passing on all traffic between them and making them believe they are talking directly to each other, when in actual fact the attacker is controlling the conversation. This enables the attacker to intercept all messages between the target and the host. An illustration of a MITM attack is shown below in Figure 5.

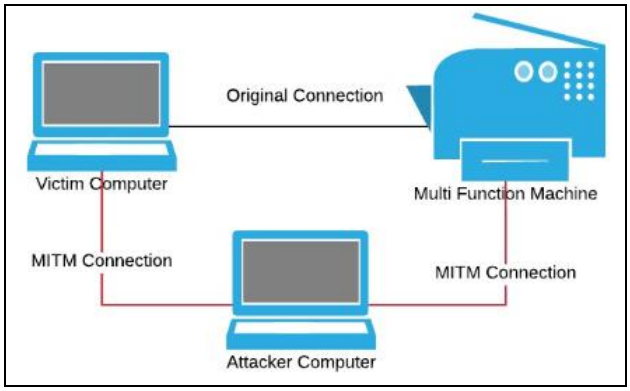

Figure 5. Diagram of a Man in the Middle (MITM) Attack Setup

Several MITM attack tools exist that can be utilised by an attacker. Some of these tools include Packet Creator[8], Ettercap[9], Dsniff[10], Cain & Abel, arpspoof[11] and Wireshark[12]. The MITM attack was not performed during this study.

4.3 Firmware Update

Researchers from the Columbia University Intrusion Detection Systems Lab were able to alter the printer firmware and successfully run the update thereof (Cui & Voris, 2011). Through the use of PJL, the firmware was updated and changed to the attacker's liking. HP LaserJet printers allow firmware updates through a process called Remote Firmware Update (RFU).

The firmware update of the HP P4015, which is a MFD used to perform tests on, was downloaded from the HP site. However, no firmware was altered in this study, but could be investigated in the future.

5. Security Measures

A range of standards, security features and secure software printing products are offered by MFD manufacturers. However, no single standard exists for MFD security. In this section an overview of security measures for MFDs is discussed.

5.1 Hard drive security

The following is recommended, by the researchers, in order to protect data stored on the printer hard drive:

- Strong data encryption is required for data stored on the hard drive.
- MFD must support the Advanced Encryption Standard (AES).
- MFDs must include functionality to erase data stored on the hard drive.
- If the device processes restricted data, it must have encryption and data overwrite functions.

5.2 Network authentication and authorisation

Network authentication is the process of validating the usernames and/or passwords on the devices. Network authentication must be employed so that users are required to authenticate at every printing task. MFDs should be set-up to handle different levels of access restrictions, such as: specific functions such as email or faxing must be limited to specific users; Only administrators should have access to the highest level of functions such as network configurations, system configurations and printing protocols; In addition, only administrators should be allowed to maintain the users stored on the MFD. Authentication over the network must be set to utilise a secure protocol. The transmission of electronic documents should have an extra layer of password protection to protect the confidentiality of email addresses.

---

[8] http://www.softpedia.com/get/Network-Tools/Network-Testing/PacketCreator.shtml
[9] http://ettercap.github.io/ettercap/
[10] www.monkey.org/~dugsong/dsniff
[11] http://linux.die.net/man/8/arpspoof
[12] www.wireshark.org

5.3 IP Filtering and Firewalls

IP filtering can be used to restrict access to the MFD to a specific range of IP addresses. IP addresses outside this range must not be granted access to the MFD. Many MFDs support the setup of Access Control Lists (ACL), which defines who can use the MFD. Enabling this feature prevents access to the web and the management interface of the MFD by unauthorised users (Geier, 2012). If the MFD is equipped with a firewall, it should be enabled. Many printers support protocols such as IPP and FTP printing as well as other features allowing users to transmit print jobs over the Internet. When these features are not utilised, they should be disabled.

5.4 MFD Administration and Management

It must be ensured that all network and administrator functions cannot be viewed or changed, both locally and remotely. The administrator password must be changed on a regular basis. The vendor documentation on security-related features and recommendations on secure installation and implementation must be reviewed on a regular basis. Regular reviews on security updates must be done.

5.5 Encryption with secure protocols

Setting up and regularly changing the administrator password might not be enough to secure the maintenance interfaces of the printer. The admin password might not be encrypted when sent from the administrator's computer to the printer, which can allow the interception thereof. Data must be encrypted as it is sent over the network to the printer. Encryption and secure protocols must be utilized to protect unauthorised access to data in transit. Secure protocols include Internet Protocol Security (IPSec), Secure Sockets Layer(SSL) v3, SNMP v3. Disable all unused management protocols such as Telnet, FTP, SSL v1, SNMP V3, SMTP, HTTPS and HTTP (University of Hawaii, 2017).

From the discussion above it is clear that a variety of security features are being incorporated into MFDs. Most of the features, however, are not enabled by default. The administrator should be aware of this and be educated when setting up the printer. Many manufacturers have placed a big focus on securing the hard drive. We regard the most problematic area as the limited security settings regarding the transmission of print jobs to the printer or print server. It is imperative to consult vendors when new devices are installed in order for users to gain the required knowledge regarding the security features of the devices.

6. Conclusion

Given the fact that multifunctional devices and standalone devices contain embedded operating systems, store data and run popular services such as HTTP, FTP and SMTP, these devices are vulnerable to hacking attacks and print data could be compromised. It has been identified that there are physical and network security risks relating to these multifunctional devices. The four main areas of vulnerabilities are physical unclaimed output, physical unauthorised access to the MFD, data that is stored on a removable hard drive and lastly network security risks. Most manufacturers release security features documents for MFDs, but many of these features are not enabled by default. Users are often not educated or aware of the security risks that comes along if a MFD is not installed securely. The cost of implementing security measures to protect a printer and the print data from being compromised are far less than the damage resulting from security risks. Therefore, it is essential to ensure that the necessary printer protection steps are followed to guarantee that the information on the printer is secured at all times.

This paper is a guideline, that can be used by administrators as well as daily users, when installing and using MFDs in a network environment, in order to ensure the devices are set-up in the best possible secure manner.

References

Acunetix. (2017). What is Cross-site Scripting and How Can You Fix it?. [online] Available at: https://www.acunetix.com/websitesecurity/cross-site-scripting/ [Accessed 28 Nov. 2017].

Baker , P. (2012) 7 Ways Criminals Could Use Your Printers to Steal Info. http://h30565.www3.hp.com/t5/Feature-Articles/7-Ways-Criminals-Could-Use-Your-Printers-to-Steal-Info/ba-p/1852

Beal, V. (2017). Webopedia.com - What is LPD/LPR? Webopedia Definition.Available at: https://www.webopedia.com/TERM/L/LPD_LPR.html [Accessed 23 Nov. 2017].

Brother Solutions Center. (2017) Using the TELNET console to configure the IP address. Available at: http://solutions.brother.com/Library/ug/mfc665cw/as-en/html/nug/appendix11_2_6.html, [Accessed 3 Aug. 2017]

Capital Document Solutions. (2013). Are Your Printers a Security Risk? Think Print, Think Security. Available at: https://www.capital-solutions.co.uk/are-your-printers-a-security-risk/ [Accessed 24 Sep. 2017].

Cbsnews.com. (2017). Digital Photocopiers Loaded With Secrets. Available at: https://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/ [Accessed 22 Nov. 2017].

Condon , E., Cummins , E., Cukier, Z. & Afoulki, M. "How secure are networked office devices?," in IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), IEEE Computer Societ, 2011, pp. 465-472.

Crenshaw, A. (2017). Irongeek.com. Hacking Network Printers (Mostly HP JetDirects, but a little info on the Ricoh Savins). Available at: http://www.irongeek.com/i.php?page=security/networkprinterhacking [Accessed 22 Nov. 2017].

Cui, A. and Voris, J.A., 2011. Print Me If You Dare: Firmware Modification Attacks and the Rise of Printer Malware. In the Proceedings of the 28th Chaos Communication Congress, Berlin, Germany.

Docstore.mik.ua. (2017). File Transfer, File Sharing, and Printing (Building Internet Firewalls, 2nd Edition). [online] Available at: https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch17_01.htm [Accessed 23 Nov. 2017].

Dotson, J. (2017). HTTP vs. HTTPS: What's the Difference?. [online] BizTech. Available at: https://biztechmagazine.com/article/2007/07/http-vs-https [Accessed 23 Nov. 2017].

Fei, Y., Jones, J., Lakkas, K. and Zheng, Y., 2002. Measurement of the usage of several secure Internet protocols from Internet traces. Student Project, Department of Computer Science and Engineering, University of California, San Diego, CA, USA.

Forbes.com. (2017a). Forbes Welcome. [online] Available at: https://www.forbes.com/sites/ciocentral/2013/02/07/the-hidden-it-security-threat-multifunction-printers/#5d208655b615 [Accessed 23 Nov. 2017].

Forbes.com. (2017b). Forbes Welcome. Available at: https://www.forbes.com/sites/alexknapp/2011/12/26/hp-releases-firmware-update-to-prevent-printer-hacking/#b286aa97035e [Accessed 22 Nov. 2017].

Geier, E. (2012) Your Printer Could Be a Security Sore Spot. Available at: http://www.pcworld.com/article/254518/your printer could be a security sore spot.html, [Accessed 23 Oct. 2017].

Gene Michael Stover, Printer Hacking., 2004.

Gromek, M. (2002). SANS Institute. Securing FTP Authentication. Available at: https://www.sans.org/reading-room/whitepapers/protocols/securing-ftp-authentication-374. [Accessed 3 November. 2017].

Hewlett-Packard (2003). HP PCL/PJL Technical Reference. Printer Job Language Technical Reference Manual. Available at: http://h10032.www1.hp.com/ctg/Manual/bpl13208.pdf. [Accessed 22 Nov. 2017].

Howtogeek.com. (2011). What Is Postscript? What Does It Have to Do With My Printer?. Available at: https://www.howtogeek.com/100016/printing-what-is-postscript/ [Accessed 22 Nov. 2017].

HP Support document. HP Color LaserJet and LaserJet Series Printers - History of Printer Command Language (PCL).

InfoSec Resources. (2015). Exploiting Corporate Printers. [online] Available at: http://resources.infosecinstitute.com/exploiting-corporate-printers/#gref [Accessed 28 Nov. 2017].

Kassner, M. (2010). TechRepublic - The truth about copier hard drives: Tips for securing your data. Available at: https://www.techrepublic.com/blog/it-security/the-truth-about-copier-hard-drives-tips-for-securing-your-data/ [Accessed 23 Nov. 2017].

Kirda, E., Kruegel, C., Vigna, G. and Jovanovic, N., 2006, April. Noxes: a client-side solution for mitigating cross-site scripting attacks. In Proceedings of the 2006 ACM symposium on Applied computing (pp. 330-337). ACM.

Konica Minolta. (2010) Bizhub C280 General Specifications. Available at: http://www.nova.edu/cwis/bsv/copy/forms/bizhub_c280_spec_sheet.pdf Accessed 23 Oct. 2017].

Konica Minolta Business Solutions. (2017). Information Security Services & Solutions. Available at: http://kmbs.konicaminolta.us/kmbs/information-management/security-compliance [Accessed 13 Oct. 2017].

Microsoft. (2017). MS01-031: Handle Leak in Telnet Service Causes a Denial-of-Service Vulnerability. Available at: http://support.microsoft.com/kb/300905, [Accessed 22 Nov. 2017].

Mirkovic, J., Dietrich, S., Dittrich, D. and Reiher, P., 2004. Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security).

Piriform.com. (2017). Recuva - Restore deleted files, even if you've emptied the Recycle bin! - Piriform. Available at: http://www.piriform.com/recuva [Accessed 22 Nov. 2017].

Rouse, M. (2007). IoT Agenda - What is man-in-the-middle attack (MitM)? - Definition from WhatIs.com. Available at: http://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM [Accessed 23 Nov. 2017].

Rubens, P. (2012) How to Securely Delete Data from Hard Drives. [Online]. Available: http://www.esecurityplanet.com/windows-security/how-to-securely-delete-data-from-hard-drives.html, [Accessed 23 Oct. 2017].

Salvatore Stolfo Ang Cui, "Print Me If You Dare: Firmware Modification Attacks and the Rise of Printer Malware," in 28th Chaos Communication Congress, Berlin, Germany, 2011.

SANS Internet Storm Center. (2017). Multiple vulnerabilities discovered in popular printer models - SANS Internet Storm Center . Available at: https://isc.sans.edu/forums/diary/Multiple+vulnerabilities+discovered+in+popular+printer+models/22023/ [Accessed 23 Nov. 2017].

Sullivan , B. (2011) Millions of printers open to devastating hack attack. http://redtape.nbcnews.com/_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack-researchers-say, [Accessed 11 November. 2017]

Support.hp.com. (2017a). HP Jetdirect and Embedded Jetdirect Inside Print Servers - How to Determine, Reset, and Configure an IP Address on an HP Jetdirect Print Server | HP® Customer Support. [online] Available at: https://support.hp.com/us-en/document/bpj02738 [Accessed 23 Nov. 2017].

Support.hp.com. (2017b). HP LaserJet M5025 and M5035 MFP Series - HP Embedded Web Server | HP® Customer Support. Available at: https://support.hp.com/rs-en/document/c00790051 [Accessed 24 Nov. 2017].

Technet. (2011) Telnet script to change admin password on Printers. Available at: http://social.technet.microsoft.com/Forums/scriptcenter/en-US/bf59b6a8-08cd-4f76-b659-55dc876a3517/telnet-script-to-change-admin-password-on-printers, [Accessed 5 Oct. 2017].

Technet.microsoft.com. (2017). What Is SNMP?: Simple Network Management Protocol (SNMP); Services for Macintosh. Available at: https://technet.microsoft.com/en-us/library/cc776379(v=ws.10).aspx [Accessed 1 Oct. 2017].

Tools.ietf.org. (2017). RFC 2911 - Internet Printing Protocol/1.1: Model and Semantics. [online] Available at: https://tools.ietf.org/html/rfc2911 [Accessed 23 Nov. 2017].

University of Hawaii, I. (2017). Securing Network Printers and Multi-Function Devices :: ASK US, University of Hawaii System. [online] Hawaii.edu. Available at: http://www.hawaii.edu/askus/1357 [Accessed 24 Nov. 2017].

Vail, V.T. (2003). Printer Insecurity: Is it Really an Issue?. SANS Institute InfoSec Reading Room, pp.1-12. Available at: http://www.sans.org/reading_room/whitepapers/threats/printer-insecurity-issue_1149. [Accessed 30 Sep. 2017].

Vijayan , J. (2011) HP LaserJet printers vulnerable to attacks. http://www.computerworld.com/s/article/9222254/HP_LaserJet_printers_vulnerable_to_attacks_researchers_warn, [Accessed 3 November. 2017]

Ward, A. (2005) The CUPS printing system. Available at: http://www.linuxjournal.com/article/8618, [Accessed 10 Oct. 2017].