Cyber Security Threats and Mitigation Techniques for Multifunctional Devices

VINEETH JOE PRADEEP J[1] , A VAISHALLI[2]

[1.2] *Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India*

ABSTRACT

Representatives of all little, small or undertaking associations make utilization of printers, copiers, scanners, faxes and multifunctional gadgets for everyday operational elements of the association. These gadgets are either out-properly acquired or got on a rent contract. At the point when the gadget's End-of-Life is achieved, the gadgets are either discarded, at times through gifts to non-benefit associations, or retuned back to the Original Equipment Manufacturer (OEM) toward the finish of a rent assentation contract. Obscure to most IT activities work force and data security faculty, these gadgets convey an inborn weakness. These gadgets have secure and unsecure organize interchanges conventions; hard circle drives; unstable memory; and non-unpredictable memory. Every one of these gadgets are defenseless against digital dangers and assaults. This paper points, to share the degree to which the association can uncover touchy data having a place with either an association or its workers if a gadget is removed off; returned back to the OEM or an assailant accesses the gadget either physical or through the system on which these gadgets dwells. This paper depends on look into that was directed on these gadgets. This paper finishes up with rules on the best way to securely utilize and decommission such gadgets to go around the loss of touchy data.

Keyword : — *Multifunctional Gadgets, Copiers, Fax, Hard Disk Drive, Memory, Vulnerability, OEM, Decommission.*

1. INTRODUCTION

Copiers, printers, and other Multifunctional Devices (MFDs) are astute gadgets that contain non-unstable memory, unpredictable memory and Hard Disk Drives (HDDs) where picture information is composed amid work preparing. It is evaluated that toward the finish of the existence cycle of a MFD that it might contain around 125,000 pages of content on its HDD. This is a lot of touchy data that can be recovered from these MFDs. MFDs regularly utilize a First-in-First-out (FIFO) model to execute occupations sent to them except if the need of a vocation is expanded. At the point when information is sent to the MFD, while different occupations are in progress, the new activity is incidentally put away in the line until the point when employments with higher needs are finished or until the point when the new activity is next in line to be executed by the FIFO arrange. This causes the whole recently began print employment to live on the capacity media and the print occupation may be recoverable by an assailant from the capacity media. The greatest guilty party to the issue is work data put away when utilizing secure print post boxes. This is an element which empowers a client to print to this 'letter drop' and just when the client lands at the printer and sorts in their stick code, at exactly that point does the activity get executed. This enables one to guarantee that the record is just printed when the client are available at the gadget, in any case, this security choice stores the print employment to the HDD until the point when the client touches base at the printer. The capacity mediums on the hardware should be cleaned before any gear is arranged, unloaded or given. It represents a digital security hazard if the substitution methodology isn't accurately performed and the old gear's HDD isn't effectively purified.

Makers of MFD gadgets have understood the dangers related with unapproved recuperation of the picture information put away on non-unpredictable memory, unstable memory and HDDs drives. Distinctive gadgets speak to various dangers relying upon the measure of unpredictable memory and HDD estimate. Not all gadgets have HDDs and some that do have HDDs don't utilize the HDDs to store picture information amid work preparing, for such sellers these gadgets don't represent a security hazard as far as unapproved recuperation of picture information. For gadgets that have HDDs and utilize these HDDs drives to store picture information amid handling, these

merchants have components and instruments set up to overwrite these drives either after each employment, when the gadget overseer so picks, or toward the finish of the rent time frame. HDD encryption is likewise included as an additional safety effort to control the unapproved recuperation of picture information from the HDD. A vital point to observe is that a considerable lot of these highlights are accessible on the gadgets, anyway they are:

• Not plant empowered and in this way should be empowered by a manager at times just at the underlying setup of the gadget;

• Or are processing plant empowered with default settings and qualifications.

Figure 1 demonstrates the MFD assault vectors, which are unapproved get to, yield protection, held data and system vulnerabilities. An unapproved get to helplessness happens when an aggressor increases physical access to the print room or print region and evacuates the HDDs of the MFDs. System vulnerabilities is the point at which an aggressor makes utilization of the MFD's system interfaces to acquire the data on the gadget. Yield protection vulnerabilities happen when an aggressor increases physical access to the room in which the MFD is kept and takes the yield of finished employments left or uncollected by clients on the MFD's plate. Held data vulnerabilities happen when an aggressor accesses the MFD's HDD or RAM physically or through the system.

Figure 1: Multifunctional Device Information Attack Vectors

2. VULNERABLE DEVICE GROUPING

The MFDs can be categorized as one of the accompanying classes as recorded in Table 1. These gadgets are both monotone and shading. The critical data to note from the table is the helpless parts of the gadgets. Note that a wide range of gadgets have helpless segments. In this paper every one of the gadgets recorded in Table 2 will be known as MFDs.

Table 1: VULNERABLE DEVICE CATEGORISATION

Device Type	User Count	Possible Vulnerable Components
Small Device	Between 1 to 5 users	RAM and Network
Midrange Device	Between 6 to 25 users	RAM and Network
Large Workgroup Device	Over 25 users	RAM, HDD and Network
Small MFD	Between 1 to 5 users	RAM and Network
Medium MFD	Between 6 to 25 users	RAM, HDD and Network
Large MFD	Over 25 users	RAM, HDD and Network

3. NETWORK ACCESS VULNERABILITIES

Numerous office gadgets have a background marked by being organized, (for example, printers) and others without the same past are progressively getting to be arranged, (for example, scanners). The cutting edge arranged adaptations of already non-organized gadgets have much in the same manner as conventional arranged servers regarding highlights and capacities. While an association may have strategies and systems for anchoring conventional system servers, anchoring information on MFDs can be not entirely obvious.

MFDs that are arranged incorporate some sort of system interface and fundamental working framework. Now and again, the working framework is like the working frameworks running on customary PCs with a prerequisite for organize availability

Table 2: Depicts the typical ports that are used for network communication on MFDs

TCP Port	Potential network service listening
21	FTP (file transfer protocol)
22	SSH (secure shell)
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
80/8080	HTTP (Hypertext Transfer Protocol)
443	Hyper Text Transfer Protocol Secure
514	RSH (remote shell)
515	LPD (line printer daemon)
9100	HP JetDirect (pdl-datastream)

4. HDD VULNERABILITIES

As per Table 1, MFD's ordinarily have a capacity HDD. This enables the client to file reports to the hard drive for later printing. Accidentally, the gadgets likewise utilizes this stockpiling when it gets substantial employments that should be put into a line. On the off chance that the gadget's HDD is in an unreliable room which has physical access, which is ordinarily the case because of the average utilization of such a gadget, the capacity media can be evacuated by an aggressor. The procedure on the best way to expel this stockpiling media is all around recorded, in the administration manual of the gadget, and is accessible on the web and normally just requires a screwdriver.

5. RAM VULNERABILITIES

In all cases the devices summarized in Table 1 use RAM to temporarily store documents on. These devices with RAM that use RAM to store documents can be plugged into a network in for weeks holding documents data in RAM. From an administrative perspective it is possible to re-execute jobs that are stored in the RAM. Therefore it is important from time to time to clear the RAM by powering off the MFD completely for a defined period of time. This is because RAM is volatile memory meaning, once the device is turned off, and in some cases taking the power out of the socket wall for a few minutes, manufacturers of some of these devices consider the security threat posed by the jobs stored in RAM as eliminated.

6. DATA RECOVERY ON AN MFD

This segment depicts strategies that can be utilized to get delicate data from a MFD. It is accepted that the MFD has a HDD or system interface card that is associated with the web.

A. Step by step instructions to Retrieve Data from the HDD of a helpless

MFD

Typically the room that stores the MFD is left open for simple entry and in most professional workplaces with an open arrangement office, anybody can get to the MFD. It is fascinating to take note of that notwithstanding for official administration, it is conceivable to access the MFD gadgets they utilize. An assailant could be a noxious insider or the aggressor could utilize social designing to access the open arrangement office including the print region or room. Once inside and remaining beside the MFD, it is feasible for the assailant to get to the picture information store on a MFD's HDD amid work handling by physically expelling the MFD's HDD and far from the scene of the wrongdoing the aggressor would then interface the HDD into his/her PC.

On the off chance that the HDD of a MFD is evacuated the accompanying presumptions must apply all together for the aggressor to approach the printed information in particular: x No encryption or frail encryption on the HDD; x No secret key on the HDD; x No overwrite on the HDD.

Once the MFD's HDD is in the ownership of the aggressor, and the above conditions and suppositions are valid. The assailant can utilize a plenty of instruments to right off the bat get to delicate data on the HDD and furthermore to recuperate information that was beforehand erased from the HDD. Figure 2 demonstrates one such apparatus, to be specific FTK Imager that is unreservedly accessible on the web and can be utilized to mount the HDD and to see its substance. This instrument, as

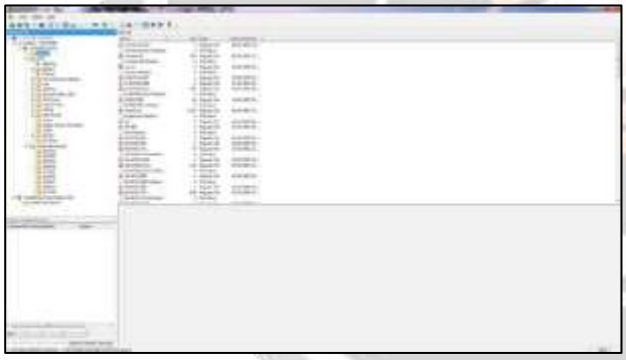

Figure 2: MFD Data viewing using FTK Imager

The scientists found that each instrument that can be utilized to see and recuperate information from a HDD utilizes distinctive calculations. Every instrument can recover information or documents that the others can't.

B. How to recover information from an Encrypted MFD's HDD

In an examination article by Lee et al (2011) an examination was performed to perceive what can be recuperated from a MFD's HDD [6]. The HDD had four segments on it. The main parcel had a review log which is recorded in plain content. Despite the fact that encryption is turned on, there is no encryption on the review log. The review log contains data, for example, startup occasion, shutdown occasion, print work occasion, filter work occasion and security setting occasion. Lee et al (2001) first made an endeavor to recuperate an archive that was printed utilizing the protected printing work usefulness to which they were not able recoup the report straightforwardly, yet they were effective in separating the ID, secret word and the filename.

Utilizing the data about the protected printing work, the scrambled document was recuperated. The scientists were not able unscramble the document, be that as it may, the record was duplicated off the capacity gadget onto another

capacity gadget. The second stockpiling gadget was then associated with a MFD. Utilizing the usefulness of the MFD the safe printing employment could be restarted and the scrambled report could be re-printed utilizing the secret word acquired.

Figure 3: demonstrates a correlation of the first print work and the

C. How to Retrieve information from Vulnerable MFDs over the system

It is conceivable to get to the picture information put away on a MFD

HDD amid work preparing through a system association.

Figure 4: demonstrates the five phases of hacking that an aggressor could influence utilization of keeping in mind the end goal to discover To mfd gadgets that have organize

As indicated by Figure 4 the initial two stages an aggressor would do is to first accumulate data about the objective on the Internet, after which, the assailant plays out an inactive output of the objective by checking for open ports. There are for the most part two noteworthy sites that an aggressor could utilize, the first being Google.com and the second being Shodan.io. In this paper just the Shodan.io site seek strategy is illustrated.

By signing into shadon.io and entering "country:ZA port:9100" it conceivable to discover powerless gadgets that are MFDs and have the 9100 port open in South Africa. This string can be additionally enhanced to incorporate the name of a particular item, for example, Ricoh, Lexmark, HP, and so forth and the name of the objective orgnisation. The refreshed hunt string would then be: "country:ZA port:9100 product:ricoh org:<name of target organisation>". Utilizing this hunt string would bring about the assailant seeing whether the objective association has powerless gadgets that can be abused.

Figure 5: demonstrates the aftereffects of running the above question on Shodan.io. The IP locations of the helpless gadgets can be seen and their areas. By playing out a brisk peruse on the objective association's site an assailant can rapidly acquire area of the head office of the objective association. The assailant would then scan for gadget in the suburb in which the objective association's head office is. Once an IP address is found there, the assailant would then get the client manual for the

Normally the username and watchword of the gadgets are:

x Username as Administrator or Admin and the secret word as <blank>.

x Username as Admin or Administrator and the secret key as administrator.

Once the assailant has effectively signed on the gadget, the aggressor can explore to the report picture stockpiling of the

Shodan.io depends on open ports on the MFD. These ports can be closed off behind a corporate firewall, in any case, it is as yet essential to know about these vulnerabilities. Because the ports are closed off on the firewall, the plain same vulnerabilities can be misused from inside the system [7] [8]. It is imperative to endeavor to relieve any potential vulnerabilities previously they happen. The accompanying segment talks about a few moderation procedures as gave by the diverse MFD producers.

7. CONCLUSIONS

MFDs that are associated with the Internet are powerless against fundamental assaults, except if legitimate care has been taken to anchor these gadgets, for example, changing default passwords, empowering picture information auto-cancellation, incapacitating putting away picture information onto the MFD's HDD amid work preparing where conceivable, scrambling the MFD's HDD, setting a secret key on the HDD, square MFD ports that not being utilized, and so forth. For MFDs that don't have the above set up it is conceivable to look for them, login into their authoritative records utilizing default certifications and survey the picture information as well as having the capacity to recoup that picture information. This is on account of MFDs have HDDs that are the same to standard PC drives. Standard PC drives don't erase information put away on them when the information is erased or the HDD is designed utilizing standard organizing systems. By utilizing a mix of free devices and exclusive instruments, it is conceivable to not just view beforehand erased information on a HDD yet to likewise recuperation already erased information.

8. FUTURE WORK

The researchers suggest that every association ought to assess the relief systems as depict in Section VII with a specific end goal to assess whether the gadgets utilized as a part of their condition are helpless against data misfortune. This is on account of MFD producers each have distinctive techniques to avoid against information misfortune on their MFDs. The scientists were additionally not ready to decide the data that is put away in a MFD's RAM memory and if that data is erased after the MFD has been killed then on once more.

9. REFERENCES

[1] Bilello, C. (2017). Hard Drive Data Security. (Konica Minolta) Retrieved October 24, 2017, from https://www.uwyo.edu/auxserv/copier- services/konicaminoltahddsecuritymay2010compatibilitymode.pdf

[2] Business Technology Association. (2012, September). Vendor Data Security Q & A. (Business Technology Association) Retrieved October 30, 2017, from http://www.bta.org/page/VendorSecurityQA

[3] Freed, N. (2000, October). Behavior of and Requirements for Internet Firewalls. Retrieved from The Internet Society (2000): https://tools.ietf.org/pdf/rfc2979.pdf

[4] Garrard, D. L. (2003, July). A Security Assessment of the Ricoh Afcio 450E Multifunction Device. (SANS Institute) Retrieved October 30, 2017, from https://www.sans.org/reading-room/whitepapers/networkdevs/security-assessment-ricoh-afcio-450e- multifunction-device-1211

[5] Hernandez, J., Sierra, J., Gonzalez-Tablas, A., & Orfila, A. (2001, Oct). Printers are dangerous. Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186), pp. 190-196.

[6] James, D. (n.d.). The Corporate Risks Associated with Obsolete Computer Equipment. (InfoSecWriters) Retrieved Oct 30, 2017, from http://www.infosecwriters.com/Papers/DJames_Obsolete_Computers.pd f

[7] Kyocera. (2017). Data Security Kits for Printers and Multifunctionals. (Kyocera) Retrieved October 24, 2017, from Data Security Kits for Printers and Multifunctionals

[8] Lee, K., Lee, C., Park , N., Kim, S., & Wo, D. (2011). An Analysis of Multi-function Peripheral with a Digital Forensics Perspective.

[9] Lexmark. (2017). Hard Disk Security. (Lexmark) Retrieved October 24, 2017, from https://www.lexmark.com/en_xc/solutions/security/hard- disk-security.html

[10] Lukusa, J.-P. K. (2016, May 18-20). A Security Model for Mitigating Multifunction Network Printers Vulnerabilities. Proceedings of the 1st International Conference on the Internet, Cyber Security, and Information Systems (ICICIS), Gaborone. Retrieved from https://www.researchgate.net/profile/Jean_Pierre_Lukusa/publication/303382654_A_Security_Model_for_Mitigating_Multifunction_Network_Printers_Vulnerabilities/links/573f64a108ae9f741b321e5d.pdf