Security Analysis of the MIT Pharos Printing Network

Emily Do emilyhdo@mit.edu

Huy Pham huypham@mit.edu

Preksha Naik prekshan@mit.edu

6.857 - Computer and Network Security, Spring 2016

Athena printing quota: ∞

Abstract

We performed a security analysis of the MIT Pharos Printing network, a centralized printing service that was deployed in 2011 by IS&T. Specifically, we established four criteria we thought most necessary to maintain a secure printing network: (i) prevent unauthorized control and configuration of the printers, (ii) prevent sensitive user data from being accessible (iii) prevent abuse of the printing service (e.g. free printing, lack of user authentication), and (iv) prevent misuse of system components. We investigated and determined vulnerabilities in the MIT Pharos Printing network along the lines of these four criteria.

1 Introduction

Network printers enable multiple devices and multiple printers across a common wireless network to connect. MIT makes use of Pharos, a proprietary system, that centralizes the MIT Printing network. Prior to MIT deploying this system, users had to specify the printer name to which to send documents. After this, the user had to go to the specified printer in order to retrieve the document.

The Pharos software package provides ”hold-and-release” printing. Under this system, from the user's perspective, when a document is printed, the document can be retrieved by the user at any release station. A release station is a printer and a corresponding card reader. When a user scans his/her ID card at the reader, a list of documents that the user has sent appear on the card reader screen. At this point, the user can select the documents to be printed and retrieve them from the associated printer.

The goal of this project was to perform a security analysis of the MIT Pharos printing network. In this paper, we highlight past work on network printers, outline the architecture of the MIT printing network, detail our investigation and resulting vulnerabilities found within the system, and conclude by providing suggestions for best securing the network.

2 Background

Past work done on investigating the security of network printers is varied both in terms of vulnerabilities discovered and types of printers investigated. In this section, we detail three sources of past work and research we found most useful in the course of our investigation. We looked at other studies as well, but given that a majority of the printers within the MIT system are HP LaserJets, we chose to focus on papers that studied HP printers.

2.1 Adrian Crenshaw - ”Hacking Network Printers”(2)

Adrian Crenshaw details his attempts to expose vulnerabilities within network printers. His attacks focus primarily on HP Jet Directs. The first set of attacks deal with using Simple Network Management Protocol(SNMP) to accrue information about the printers. For example, many HP JetDirects leave the SNMP community read-only name[1] to the default ”public”. This means a simple SNMP walk can reveal information about the configuration of the printer, including MAC addresses, revision numbers, printer settings, etc. Furthermore, many of his attacks are feasible because port 9100 (the standard TCP port used by many HP printers for data transfer) is left unprotected. One simple but harmless attack includes changing the LCD display of the printer. Another makes use of a tool called HiJetter, which provides direct access to a variety of ports in HP printers. Through the use of this tool, one of the attacks is to treat the printer like a file server (e.g. transferring large files to the printers hard drive.) Crenshaw also discusses a vulnerability in version 7.0 of Pharos(the current version used by MIT is 8.4) where the recently completed print jobs are saved temporarily on the printer and can be seen by anyone using the printer. Crenshaw, however, notes that a patch for this was released by Pharos. We used Crenshaw's research as a starting point for our investigation and tried to see if the same attacks could be applied to the MIT printing network. Our results are discussed in section 4.

2.2 Cui et al. - ”When Firmware Modifications Attack”(4)(7)

Columbia researchers were able to infect HP printers with malicious code because of a lack of authentication of firmware upgrades. The attack, which the researchers term as the ”HP-RFU(Remote Firmware Update) vulnerability” involves delivering a malicious PJL[2] command to the raw-printing processing subsystem of the targeted printer. This attack was possible because the printers processed firmware upgrades by simply checking if a software update was included every time the printer accepted a job. The authenticity of the software was not verified, meaning malicious firmware coming from an adversarial source would be automatically accepted. This coupled with the fact that disabling RFU was difficult meant that that many printers were vulnerable. Furthermore, it was possible to construct the attacks such that they were undetectable by the printer's owner. For example, in one demonstration, the researchers were able to to print a tax return on an infected printer which in turn, sent the tax form to a second device, playing the role of an adversary's machine. In our investigation, we sought to determine whether similar attacks involving malicious firmware were viable within the MIT network.

2.3 Condon et al. - ”How Secure are Networked Office Devices”(6)

Condon et al. explore the security of networked office devices (specifically HP jet directs) by performing a data analysis of printers within a network address space. Namely, the researchers investigate which ports on the printers are open, if the web interfaces, telnet ports, and FTP ports are available, accessible, and/or password-protected, if the printers are accessible beyond local wireless networks, and whether printers store sent jobs on the hard drive. This analysis performed by Condon et al. aligned well with the questions we asked about the MIT printing network and help set up a framework for our investigation.

3 MIT Pharos Printing Architecture

3.1 System Components

There are five major system components in the MIT printing network: IS&T Pharos Server, TechCash Authority, omegas (card readers), printers, and users.

[1] The community name serves as a password to authenticate communication between the SNMP manager and the agent, which in this case is the printer. There exists both a read-only and a write-only community name which sets the permission with respect to these two operations.

[2] Printer Job Language (PJL) is a method developed by Hewlett-Packard for switching printer languages at the job level, and for status read-back between the printer and the host computer.

1. **IS&T Pharos Servers** The IS&T Pharos servers accept print jobs from users via the LPR (Line Printer Remote) protocol and store jobs in the database for a period of twenty-four hours. They also communicate with the omegas and the TechCash Authority to enable appropriate authentication, authorization and distribution of jobs to the printers.

2. **TechCash Authority**: The TechCash Authority keeps record of the three thousand page printing limit for each user of the system.

3. **Omegas**: Omegas are the ID card readers supplied by Pharos. The web page for the configuration of the omegas is accessible via `http://<printername>-omega.mit.edu:8080`. Most of the web pages for the omegas do not filter out user requests based on IP addresses. Furthermore, many omegas have configuration pages that are accessible via the default password, ”pharos”.

4. **Printers**: Printers in this system are supplied by HP, and most are HP LaserJets. Each printer has a name corresponding to its location (e.g. barker, w61cluster, ajax, etc.) and an associated omega. Most printers have an embedded web server that provides remote configuration for the printers. The URL for the configuration page is `http://<printername>-p.mit.edu`. In the intended security settings originally set by IS & T, most printers filter out requests based on IP address to prevent unauthorized access to the configuration page.

5. **Users**: Users are members of the MIT community. In order to use the printers, the user must scan his or her ID card at an omega. The default limit on the number of pages printable by an user is 3000.

3.2 System Overview

Next, we describe the process from the system's perspective.

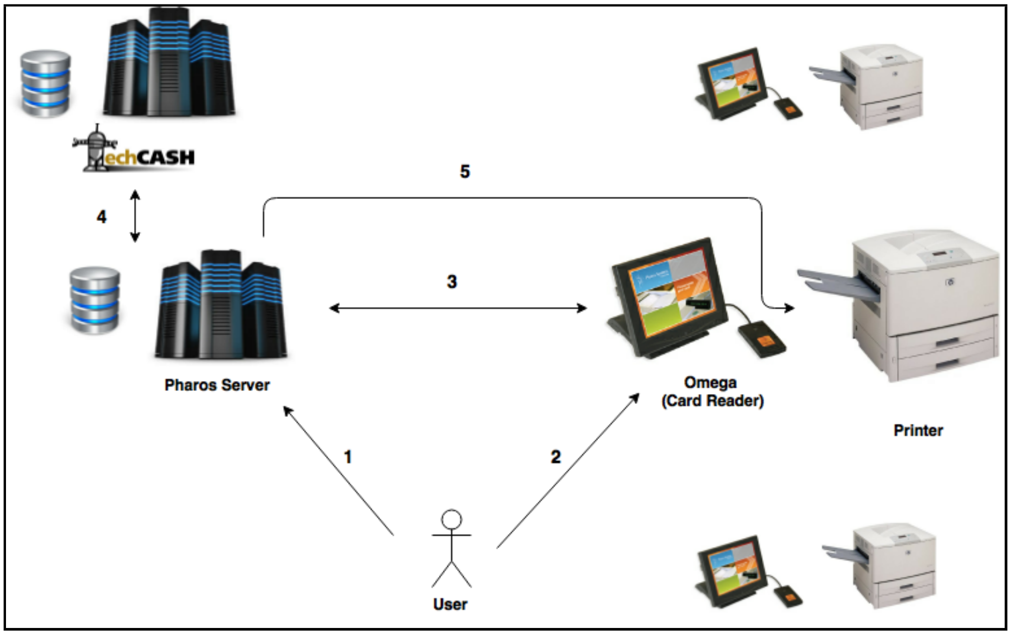


Fig. 1: Overview of the MIT printing network

1. **Users and Pharos Server**: A user sends a document using the LPR protocol to a Pharos server. A username is sent alongside the print job in plaintext. There is no authentication involved in this step. The Pharos server stores the print job in its database for twenty-four hours.

2. **Users and Omega**: In order to print the document sent to the server, the user can go to any release station on campus. Each release station is made up of a printer an an omega. After the user scans an ID card, a list of documents that the user has sent to the server appears on the omega. The user can then select the documents the user wishes to print and retrieve them from the printer.

3. **Omega and Pharos Server**: When the user scans the ID card, the omega sends the user's authentication to the Pharos server. After the user is authenticated, the server returns a list of documents it has stored in its database, corresponding to the user's username(in this case, the Kerberos on the ID card). Every time the user selects a document to print on the omega, the omega will send a message to the server indicating the document. The communication between the omega and the pharos server is encrypted.

4. **Pharos Server and TechCash Authority**: MIT students can print 3000 pages a year for free. The quota is set to avoid excessive printing from users. When the IS&T Server receives a request from a user to print a document, it first checks with the TechCash Authority to determine whether the user has reached their limit. If the user has, the TechCash Authority will deduct the corresponding number of pages printed from the user's account and send an approval message to the Pharos Server. Otherwise, it returns a message saying the user has exceeded their limit.

5. **Pharos Server and Printer**: After receiving approval from the TechCash Authority, the Pharos Server sends the print job to the printer corresponding to the omega that sent the print request. The print job is sent via wire in plaintext.

4 Security Analysis

4.1 Security Goals

We outline four goals we think are most relevant to the security of a printing network. We detail our results with respect to each to each of these goals.

1. **Prevent Unauthorized Access and Control of Printer Configuration**: An adversary should not be able to manipulate any of the settings on the printer. This includes changing the security settings, the network settings of the printer, the protocols used, etc.

2. **Prevent Unauthorized Access to User Data**: An adversary should not be able to access sensitive information of users in the printing network. This includes information about the documents submitted, ID card information, or other personal information about the user. At no point should an adversary be able to look at any of the system components and figure out this information related to the user.

3. **Prevent Abuse of Printing Service**: An adversary should not be able to use the printing service using another user's credentials. Furthermore, MIT imposes a limit of 3000 pages per user per year. An adversary should not be able to print for free or be able to exceed this limit.

4. **Prevent Misuse of System Components**: An adversary should not be able to use the printers for a purpose other than printing. An adversary should also not have the capacity to disrupt any of the system links. This includes using the printers to perform Distributed Denial of Service Attacks or spreading malware across the network computers.

4.2 Vulnerabilities

We analyzed the system with respect to each of these goals. We found significant differences between having and not having physical access to the system. Here, we discuss vulnerabilities investigated and discovered.

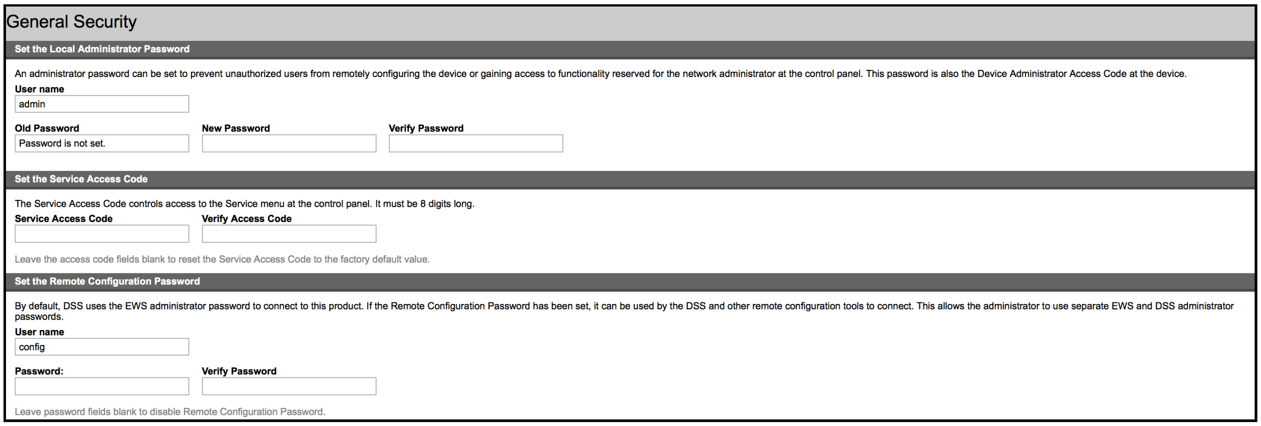
4.2.1 Unauthorized Access and Control of Printers' Configuration

Control of the printers' configuration An *nmap* scan reveals that the printers can be configured using two protocols: SNMP and HTTP.

The SNMP read-only community string in use is the default one(”public”). Therefore, anyone is able to view the configuration of the printer. However, the SNMP read-write community string, which enables someone to change the configuration settings, has been modified, thus preventing an unauthorized party from using the SNMP protocol to change the configuration.

The printers also filter out HTTP requests to access the configuration page based on IP addresses. Access to the printer's configuration page was denied on the IP addresses that we tested.

Thus, with this configuration, it is not easy for an adversary to take control of the printers' configuration. We speculate some possible attacks an adversary can potentially impose on the system. Since the SNMP protocol in use is version 2, which has no authentication or encryption, eavesdropping the SNMP signal to learn about the read-write community string is possible. In addition, as far as we know, there is no mechanism in place to limit the rate and the number of SNMP requests, thus online brute-forcing the read-write community string is possible. This method's probability of success, of course, depends on the strength of the password. Hopefully, a very strong password is set by the network administrator. Another thing worth mentioning is that if all of the printers in the network use the same password, which is likely since SNMP is mostly used for automatic configuration of network printers, an adversary with the read-write community string can control all printers in the network.



General Security

Set the Local Administrator Password

An administrator password can be set to prevent unauthorized users from remotely configuring the device or gaining access to functionality reserved for the network administrator at the control panel. This password is also the Device Administrator Access Code at the device.

User name
admin

Old Password
Password is not set.

New Password

Verify Password

Set the Service Access Code

The Service Access Code controls access to the Service menu at the control panel. It must be 8 digits long.

Service Access Code

Verify Access Code

Leave the access code fields blank to reset the Service Access Code to the factory default value.

Set the Remote Configuration Password

By default, DSS uses the EWS administrator password to connect to this product. If the Remote Configuration Password has been set, it can be used by the DSS and other remote configuration tools to connect. This allows the administrator to use separate EWS and DSS administrator passwords.

User name
config

Password:

Verify Password

Leave password fields blank to disable Remote Configuration Password.

Fig. 2: An adversary can set up an administration password, a service access code, etc.

An adversary with physical access to a printer can easily take control of the printer's configuration. He or she can simply reset the configuration of the printer using the control panel in front of the printer. This is possible because the PIN/password is not required to reset the printer. We successfully reset the configurations of two printers in the network using this method. After the reset, the adversary can access the configuration page of the printer via a web browser, which grants the adversary full control of the printer, including setting up an administrative password, changing the IP address, and installing new firmware (Fig. 2).

Control of the Omegas Configuration We are also interested in learning about the vulnerability of the omegas because they might contain data associated with the credentials of the users. The current configuration allows us to take control of the omegas.

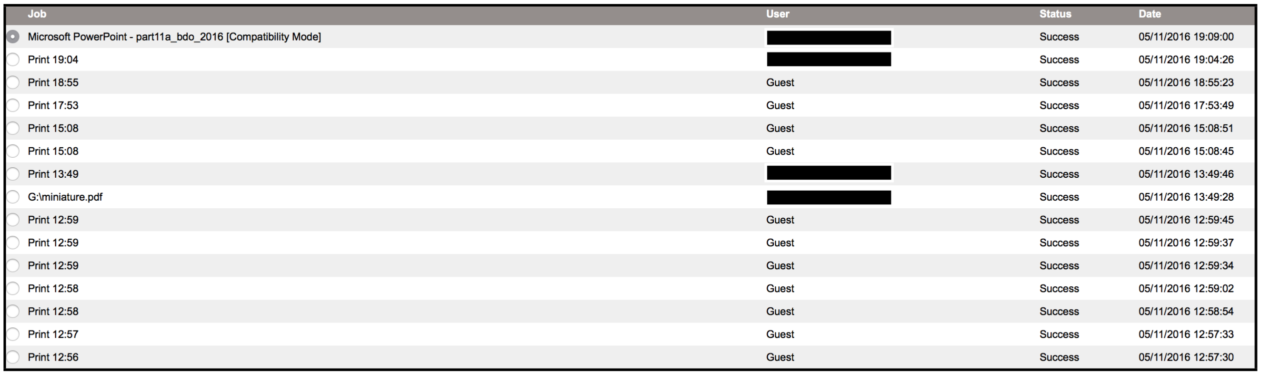
We observed a pattern in the naming of omegas and printers. Printers are named as `<printername> -p.mit.edu`. Conveniently, the corresponding omegas are named as `<printername>-omega.mit.edu`. This pattern allows us to learn the host names and IP addresses of the omegas, given the names of the printers. Moreover, the omega allows access to its configuration page using port 8080. Although it was protected with an admin password, several omegas (e.g. ajax-omega, bricks-omega, bias-omega, pulp-fiction-omega, etc.) still use the default password "pharos". Similar to the printer, after having access to the configuration page of the omega, we are able to change its IP address, see its log, change its display, etc. We did not focus on attacking the omegas because it does not store the print job data and uses a proprietary protocol and encryption for its communication.

Our observation suggests the security of the system is not centralized. We believe this discrepancy amongst the printers suggests that there is no central mechanism to authenticate and protect the printers. When a new printer is added to the network, it is either secured by an IS&T employee or comes ported with the default settings.

4.2.2 Unauthorized Access to User Data

The printers receive print job data from the Pharos servers. Although the printers do not store the data, temporary files might be in a printer's hard drive for a long period of time. The current configuration of the printers uses the Non-Secure Fast Erase mode (the least secure file erase mode) for performance. After a printer finishes printing a document, the data from the document is not overwritten. In addition, the printers' hard drives are not encrypted.

A potential attack is to take advantage of the fact that the print jobs are sent in plaintext from the Pharos servers. An adversary can potentially eavesdrop the unencrypted data.



	Job	User	Status	Date
●	Microsoft PowerPoint - part11a_bdo_2016 [Compatibility Mode]	[redacted]	Success	05/11/2016 19:09:00
○	Print 19:04	[redacted]	Success	05/11/2016 19:04:26
○	Print 18:55	Guest	Success	05/11/2016 18:55:23
○	Print 17:53	Guest	Success	05/11/2016 17:53:49
○	Print 15:08	Guest	Success	05/11/2016 15:08:51
○	Print 15:08	Guest	Success	05/11/2016 15:08:45
○	Print 13:49	[redacted]	Success	05/11/2016 13:49:46
○	G:\miniature.pdf	[redacted]	Success	05/11/2016 13:49:28
○	Print 12:59	Guest	Success	05/11/2016 12:59:45
○	Print 12:59	Guest	Success	05/11/2016 12:59:37
○	Print 12:59	Guest	Success	05/11/2016 12:59:34
○	Print 12:58	Guest	Success	05/11/2016 12:59:02
○	Print 12:58	Guest	Success	05/11/2016 12:58:54
○	Print 12:57	Guest	Success	05/11/2016 12:57:33
○	Print 12:56	Guest	Success	05/11/2016 12:57:30

Fig. 3: This shows a log of users, documents printed by the user, and the time-stamps

As we mentioned in the previous sections, taking control of the configuration of the printers is particularly easy under some circumstances. If an adversary is able to change the configuration of the printers, the number of possible attacks is endless. Having access to the configuration page of a printer allows the adversary to obtain sensitive information such as the job log of the printer (Fig. 3). More specifically, the adversary can learn names of the printed documents, usernames, when the document was printed, etc. The adversary can even obtain the content of the documents that users print. Below, we propose two possible attacks: (1) a man-in-the-middle attack and (2) an attack by installing new firmware and backdoor.

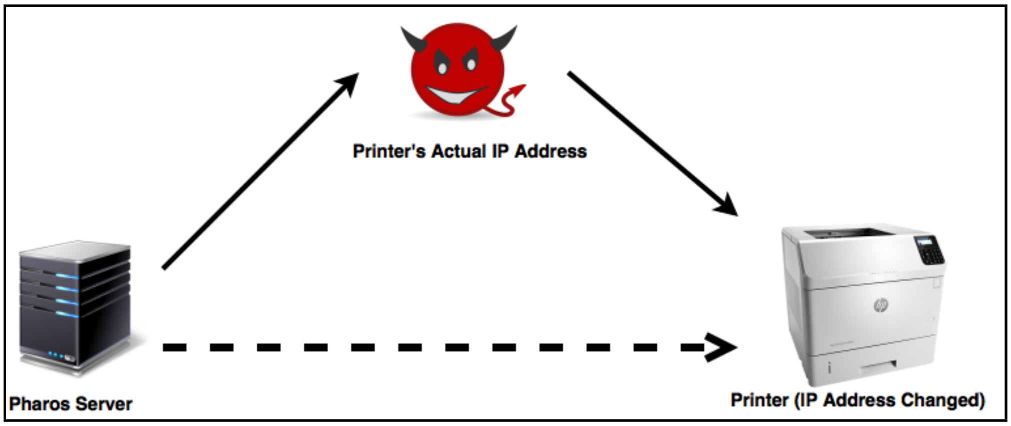
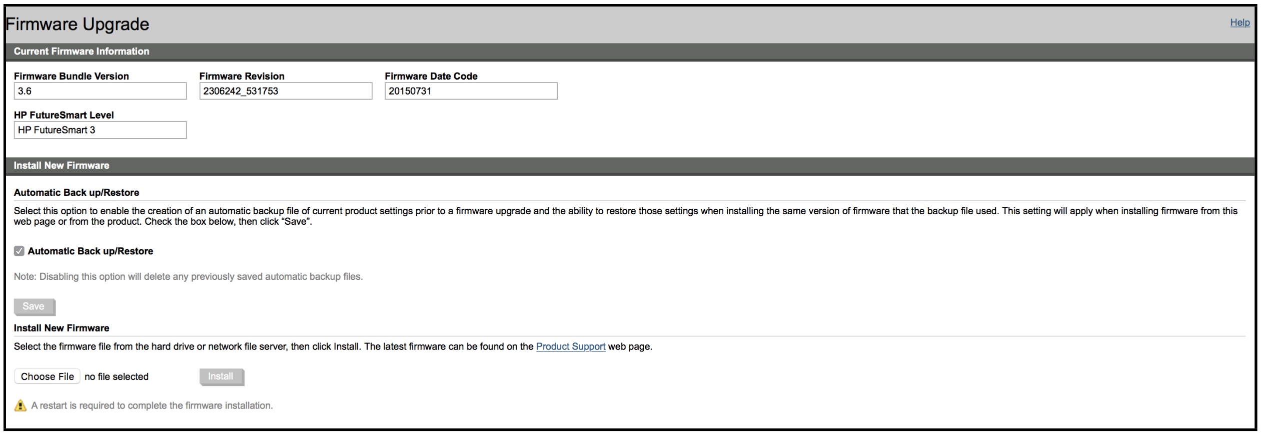


Fig. 4: Overview of the man-in-the-middle attack on the print job data



Firmware Upgrade

Current Firmware Information

Firmware Bundle Version 3.6

Firmware Revision 2306242_531753

Firmware Date Code 20150731

HP FutureSmart Level HP FutureSmart 3

Install New Firmware

Automatic Back up/Restore

Select this option to enable the creation of an automatic backup file of current product settings prior to a firmware upgrade and the ability to restore those settings when installing the same version of firmware that the backup file used. This setting will apply when installing firmware from this web page or from the product. Check the box below, then click “Save”.

☑ **Automatic Back up/Restore**

Note: Disabling this option will delete any previously saved automatic backup files.

Install New Firmware

Select the firmware file from the hard drive or network file server, then click Install. The latest firmware can be found on the Product Support web page.

no file selected

⚠ A restart is required to complete the firmware installation.

Fig. 5: An adversary can install new firmware with known vulnerabilities

1. **Man-in-the-middle attack**: Once an adversary takes control of the configuration of the printer, he/she can steal the user data by performing a man-in-the-middle attack (Fig. 4). First, the adversary changes the IP address of a targeted printer to a different IP addresses. The adversary also changes his/her own device to the real IP address of the printer. Any printer jobs intended to be sent to the printer will now be sent to the adversary. In order to avoid suspicion from users, the adversary can forward the obtained print jobs to the printer. If users do not notice any difference, the attack may go undetected.

2. **Attack by installing new firmware and backdoor**: Having control over the configuration of the printers allows the adversary to install new firmware to the printers (Fig.5). A determined attacker may look for an old version of the firmware with known vulnerability for a specific printer model, install that version, and use an exploitation tool such as Metasploit to install backdoor to the printer. At this point, the attacker has the capacity to take full control of the printer. Furthermore, the attacker can forward the print jobs that the printer received to a device controlled by the attacker in hope that the print jobs may contain sensative data.

4.2.3 Abuse of Printing Service

Authorized users, in order to use the printing service, prove their credentials by scanning their ID cards at an omega. An adversary can use the printing service by (1) pretending to be an authorized user using the users credentials or (2) fooling the system to allow printing without providing any credentials. After trying both approaches, we learn that while stealing other users' credentials is somewhat difficult, it is particularly easy to use the printing service without providing credentials.

Stealing other users' credentials As mentioned in the description of the system, the Pharos server accepts any print jobs and username without authentication. An adversary can easily send a print job with a username of an authorized user to the Pharos server. However, in order to retrieve that print job, the adversary needs to provide the credentials of the user. Assuming the adversary does not have access to the user's ID card, he or she somehow needs to obtain the credentials of the user, potentially from the omega.

Similar to the printer, the omega communicates with the Pharos server via wire. However, unlike the data between the printer and the Pharos server, ones between the omega and the server are encrypted and follow a proprietary protocol developed by Pharos. As a result, eavesdropping the signals does not directly reveal the users credentials. We found little information regard the protocol. Hence, we moved on to the second approach.

Fooling the system We learn that it is possible to use the printers without providing credentials. Below, we present two methods that an adversary can do to get free printing service.

1. **Printing from a USB drive**: MIT printers are HP LaserJets. Some of the models including HP LaserJet M605 have a USB port, which allows printing from a USB drive. Although this function is

disabled in the normal settings of the printers, one can easily enable it from the control panel. Using this method, we were able to use several printers without having to scan our ID cards at a print station.

2. **Printing remotely from a personal computer**: If the adversary has control over the configuration of the printers, he or she can remove the filters for IP addresses, allowing the printers to accept any print jobs. As a result, the adversary can remotely send the print jobs to the printers and get free printing. We succeeded in doing this after resetting a printer from the control panel. This also allows the adversary to perform a variety of attacks on the printers that we will discuss later in this paper.

4.2.4 Misuse of System Components

In this section, we consider possible attacks related to abuse of printer functionality for the adversary's purposes.

With Physical Access Once a printer's security settings have been reset, the printer is open to many vulnerabilities as the previously filtered ports of the printer are now open.

1. **Use printers as file servers** Using HiJetter, an existing tool known to provide easy access to HP LaserJets, we were able to use the printer to store individual files. Namely, we were able to take files from our local device and transfer them directly to the printer's hard drive. After deleting the files from our local system, we were able to connect using HiJetter once again and retrieve the document. This means a user can treat the printer like a temporary hard drive, both filling up the printer's capacity and abusing the printer capacity.

2. **DDoS attack**: An attacker can use the printers to perform DDoS attacks to other devices, especially devices within the MIT network or use them as pivots to compromise the security of other computers in the MIT network.

3. **Changing the display of printers and Omegas' screen**: An attacker can set what is displayed on the printers and omegas' screen. For example, we changed a printer's settings so that the screen now shows "6.857isgreat" instead of showing the IP address of the printer as default.

Without Physical Access Although the printers block requests from certain IPs, the omegas do not in the current state of security. Namely, the display on the omegas can be changed by accessing the configuration page directly. Furthermore, security can be compromised by changing any of the configurations that connect the Pharos server to the omegas.

5 Security Recommendations

Based on our investigation, we propose the following recommendations for better securing the MIT printing network.

1. **Set Control Panel Password**: Our investigation demonstrates that the greatest security vulnerability within the system is that control panel password is not enabled. This allows the adversary to reset the security of the system. This capacity enables an adversary to accomplish easily what previously was difficult including accessing configuration pages for the printer from previously filtered IP addresses, transferring data across ports that were previously blocked, and installing unpatched firmware within the printer. As a result, our first and foremost recommendation is to secure the control panel.

2. **Use a More Secure File Erase Mode**: We learned that the printers in the system are set to use the Non-secure Fast Erase mode in which files are not overwritten. Although this mode gives the best performance, it allows the adversary to potentially steal the print job data from the temporary files. We suggest IS&T set the file erase mode of the printers to be the Secure Fast Erase Mode (in which files are overwritten using one pass) for better security and still reasonable performance.

3. **Use Printers with Encryption Capability**: Printers with encryption capability helps secure data while it is transfered from the Pharos servers and the printers, protecting against an attacker with eavesdropping capability.

4. **Centralize Security Updates**: We noticed an inconsistency across printers in the network in terms of the parameters set and password used. This suggests that there is currently no central mechanism to preserve and update the security of printers across the network. We recommend that IS&T seek to minimize manual configuration and instead secure printers automatically. At any rate, avoid using default password and configuration.

5. **Omega Configuration Page**: We recommend that the omega web pages be configured such that IP addresses are filtered or at a minimum, the password is changed from the default setting. We also recommend that passwords be distinct among the different omega webpages in order to avoid an adversary gaining access to all omegas as a result of access to a single omega. Furthermore, we recommend imposing a limit on the password attempts in order to prevent brute-force attacks.

6. **Lock USB Port**: The USB port provides a simple way for an user to get free printing without being detected. We suggest that the port be locked or disabled to prevent abuse of this capacity.

6 Conclusion and Future Work

The MIT Pharos printing network trades-off convenience for security to some extent. While there are certain security mechanisms in place to prevent remote attacks, physical security is largely ignored. The security of the system is primarily based on trusting any user and any visitor on campus. Moreover, security of many of the individual components are poorly-managed and can be easily attacked by adversaries. To ensure user privacy and prevent adversaries from having the capacity to take full control of the system, security needs to be improved. The recommendations outlined in section 5 are few of the ways in which we believe security would be improved. At the very least, monitoring and management of system components and configurations should be performed regularly.

For this project, we have thoroughly investigated the security vulnerabilities of the printers and the omegas within the MIT network. For future work, security analysis of the TechCash Authority and the Pharos servers is necessary to ensure the system is secured as a whole. We suggest that future work focus on the proprietary Pharos software, protocols, and encryption. We were unable to perform this analysis as we did not have the time nor had contacted Pharos to obtain permission.

Prior to beginning our analysis, we spoke directly with an IS&T staff member, who noted that while performing the analysis, we should not violate user privacy nor disrupt and degrade the printing service. Because our findings may potentially threaten the system and it is currently uncertain what changes IS&T will implement as a result of the paper, we request that posting the paper be delayed until IS&T had a chance to review the document.

7 Acknowledgements

We are grateful to the MIT IS&T Staff, Professor Ronald Rivest, and the 6.857 Teaching Assistants for their support in our project. We would also like to thank the IS&T staff for providing a convenient printing service for the MIT Community and making this project possible.

8 References

1. ”Pharos Public Student Printing at MIT.” - IS&T Contributions - Hermes. MIT, n.d. Web. 18 Mar. 2016. Available: `<http://kb.mit.edu/confluence/display/istcontrib/Pharos+Public+Student+Printing+at+MIT>`.

2. Crenshaw, Adrian. ”Hacking Network Printers (Mostly HP JetDirects, but a Little Info on the Ricoh Savins).” Hacking Network Printers (Mostly HP JetDirects, but a Little Info on the Ricoh Savins). Irongeek,n.d.Web.18Mar.2016. Available: <http://www.irongeek.com/i.php?-page=security%2Fnetworkprinterhacking>.

3. Heiland, Deral. From Printer To Pwnd: Leveraging Multifunction Printers During Penetration Testing(n.d.):n.pag.Defcon.Web. Available:<https://www.defcon.org/images/defcon-19/dc-19-presentations/Heiland/DEFCON-19-Heiland-Printer-To-Pwnd.pdf>.

4. Sullivan, Bob. ”Exclusive: Millions of Printers Open to Devastating Hack Attack, Researchers Say -NBCNews.”NBCNews.NBC,n.d.Web.18Mar.2016. Available:<http://www.nbcnews.com/business/consumer/exclusive-millions-printers-open-devastating-hack-attack-researchers-say-f118851>.

5. Constatin, Lucian. ”Samsung Printers Contain Hardcoded Backdoor Account, US-CERT Warns.” CSO.N.p.,27Nov.2012.Web.18Mar.2016. Available:<http://www.pcworld.com/article/2017295/samsung-printers-contain-hardcoded-backdoor-account-uscert-warns.html>.

6. Condon, Edward, Zaina Afoulki, Emily Cummins, and Michel Cukier. ”How Secure Are Networked Office Devices?” IEEE Xplore. N.p., 2011. Web. 11 May 2016. Available:<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5958259&tag=1>

7. Cui, Ang. ”When Firmware Modifications Attack: A Case Study of Embedded Exploitation.” When Firmware Modifications Attack: A Case Study of Embedded Exploitation (n.d.): n. pag. Internetsociety. Columbia University. Web. 11 May 2016.Available: <http://www.internetsociety.org/sites/default/files/03_4_0.pdf>.