Technical Disclosure Commons

Defensive Publications Series

August 20, 2019

ALERT THE USER ON UNSECURE PRINT

HP INC

Alert the user on unsecure print

Abstract

Printers have become a regular household device. Printer owners or IT administrators do not see them always as fully equipped network computers. Printers sitting in one corner of the office or house and quietly going about the business of copying, printing, scanning & faxing might not seem to pose any real security threat. But hackers increasingly find them very attractive for malicious intents. So like any other networked device, if not properly managed, they can expose sensitive campus or personal data to unauthorized access and misuse.

Modern day printers support many print protocols and standards to give flexibility to the users to print the documents from various print clients. Unfortunately, not all of them are secure enough to safeguard the user's data.

Though there are many mechanisms available to secure the print data, user might not be aware of them and can put his/her data under risk.

The proposed solution is to **alert the user** of using an unsecure print job communication (whenever he does), and encourage him to use secure communication to mitigate the risk.

Problem Statement:

To support various print experiences, the printer supports multiple print protocols like Raw print, LPD, FTP, IPP, IPPS, Web Services Print, HTTPS etc. Out of these supported print protocols, many (except for IPPS, HTTPS) are unsecure. When a common user uses print functionality, they may not be even aware that they are printing over unsecure protocols. When user uses an unsecure path, an intruder can capture the network trace using any free tools like Wireshark and rebuild the entire job.

This may lead to:

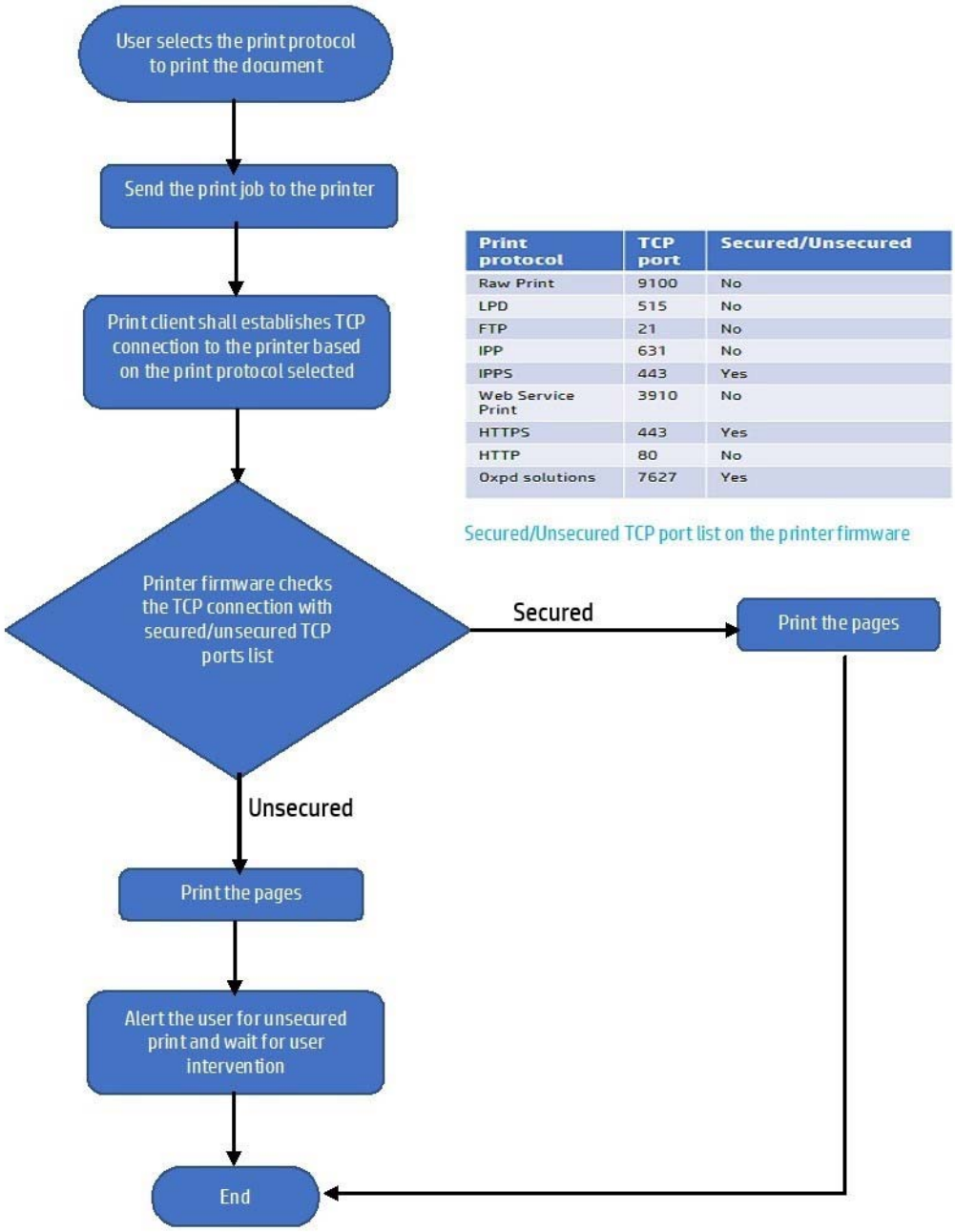
1. Unauthorized Access to Sensitive Information
2. Network Vulnerability Concerns
3. Man in the middle attacks (MITM)

Proposed Solution:

The proposed solution is for **the printer to alert the user** of using an unsecure print path for the print jobs, whenever he uses one. An alert will be displayed in the printer control panel while the unsecure job is getting printed and recommend the user to use a secure print path for future print jobs.

Printer firmware shall have the capability to know if a job is secure or not by verifying the TCP port on which it is receiving the data. For example, print data coming over 9100, 515, 631 etc., is unsecure whereas data coming over 443 is secure. Based on TCP port receiving the print job from the user, the printer can send an alert on the control panel if it's an unsecure job.

Board sequence of events could be as shown in the figure below.



Print protocol	TCP port	Secured/Unsecured
Raw Print	9100	No
LPD	515	No
FTP	21	No
IPP	631	No
IPPS	443	Yes
Web Service Print	3910	No
HTTPS	443	Yes
HTTP	80	No
Oxpd solutions	7627	Yes

Secured/Unsecured TCP port list on the printer firmware

Figure 1: Call-Flow graph for 'Alert the user on unsecure print' option

The alert can exist on the printer control panel if the job is getting printed and user intervention is required to close the alert. (Figure 2)

Alternatively, to enable or disable this solution can be given as an option on the printer web config page as a check box to "Enable alert on Unsecure Print job" and can be enabled by default.

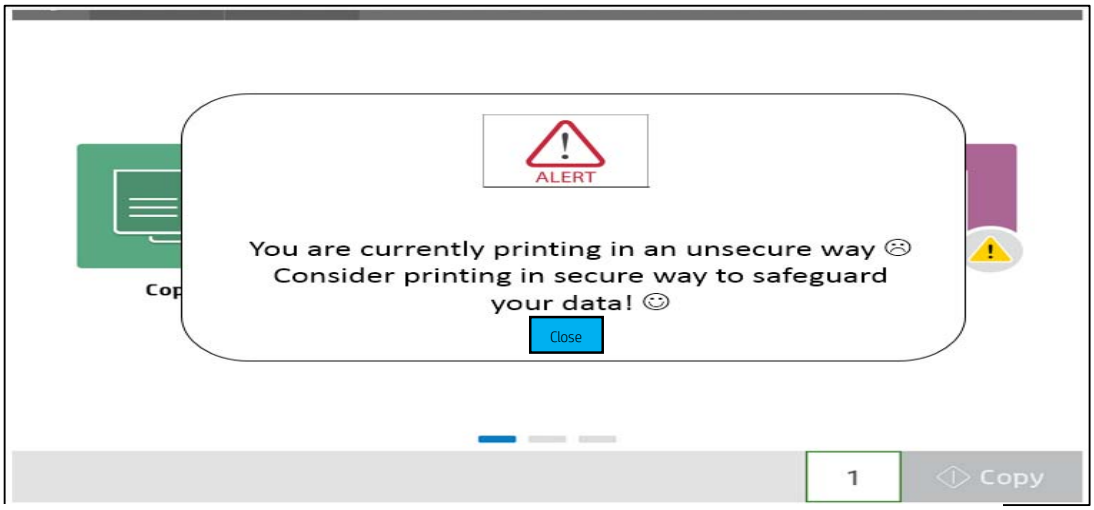


Figure 2: Control panel snapshot of the alert that will be shown while printing an unsecure job

Prior solution and its disadvantages

There is no known solutions of providing users a mechanism to know if they are using unsecure path for printing.

Advantages:

1. To secure device by minimizing the attack surface
2. Mitigate the risk of unauthorized access to sensitive information
3. Improve the availability of the printer by reducing the DoS attacks
4. This will push the security knowledge to the user which eventually make the user to take action

Disclosed by Vijaya Krishna Kotapati, Kumar Sunil, Ali Azghar Sheik and Chandrasekhar Bandi, HP Inc.