Technical Disclosure Commons

Defensive Publications Series

July 31, 2018

STORED JOBS PIN REGENERATION

HP INC

Stored Jobs PIN regeneration

Abstract

LaserJet printers provide different means of secure printing using smart cards, PIN (Personal Identification Number) etc. Print jobs secured with a PIN can be stored as a temporary or permanent file on the printer. With the current behavior on LaserJet Printers, if the user submits a PIN print job and forgets the pin, then the user can neither print the job nor delete the job. When the job resides as a permanent file, factory reset is only the option to remove the file from the printer. This paper presents a way to regenerate the PIN in a secure way to enable the user to retrieve the print file. This also reduces the need to factory reset to delete stored print files with forgotten PIN.

Solution

If the user does not collect the PIN print job and forgets the PIN, user would not have any means to recover the job. Permanent jobs never get deleted from the device storage unless a factory reset is done. Factory reset is an undesired means to clean up the stored jobs. Also, it might make user uneasy.

- Print job would carry the Email id/phone with NFC/BLE additional JOB attribute. Refer the sample PJL attributes below.

    - %-12345X@PJL JOB NAME="Microsoft Word - Doc2.docx"
    - @PJL SET STRINGCODESET=UTF8
    - @PJL COMMENT "Color LaserJet MFP M680 (15.212.10.6) (0.3.1584.18636); Windows 7 Enterprise 6.1.7601.1; Unidrv 0.3.7601.21853"
    - @PJL COMMENT "Username: gvv; App Filename: Microsoft Word - Doc2.docx; 4-10-2015"
    - @PJL COMMENT "NUP = NUP_1"
    - @PJL SET JOBATTR="OS=Windows"
    - @PJL SET JOBATTR="OS Version=Windows 7 Enterprise 6.1.7601.1"
    - @PJL SET JOBATTR="Render Type=UPD"
    - @PJL SET JOBATTR="Render Name=HP Universal Printing PCL 6"
    - @PJL SET JOBATTR="Render Version=61.175.1.18636"
    - @PJL SET JOBATTR="JobAcct1=gvv"
    - @PJL SET JOBATTR="JobAcct2=BLRSTNETDEV236"
    - @PJL SET JOBATTR="JobAcct3=ASIAPACIFIC"
    - @PJL SET JOBATTR="JobAcct4=20150410175121"
    - @PJL SET JOBATTR="JobAcct5=acb4226a-4523-4c9e-a2ea-0d9ef9f1a666"
    - @PJL SET JOBATTR="JobAcct7=splwow64.exe"
    - @PJL SET JOBATTR="JobAcct8=gvv"
    - @PJL SET JOBATTR="JobAcct9="
    - @PJL SET JOBATTR="email:gvv@XX.com"
    - @PJL SET JOBATTR="mobile:+xx xxxxxxxxx”
    - @PJL SET RET=ON
    - @PJL DMINFO ASCIIHEX="0400040101020D10100115323031353034313031323231323 1"
    - @PJL SET PLANESINUSE=1
    - @PJL SET GRAYSCALE=COMPOSITE
    - @PJL SET HOLD=STORE
    - @PJL SET HOLDTYPE=PRIVATE
    - @PJL SET HOLDKEY="1111"

- When the user prints the PIN print job, printer will generate hash of the PIN and store the below attributes.
    - User name
    - Email id/phone with NFC/BLE.
    - Job name
    - Generated hash.
- Device can provide an additional option to regenerate the PIN when maximum PIN retry limit is reached. Maximum PIN retry to regenerate the PIN can be configured say 3.
- User can agree or deny regenerating the PIN.
- If the user denies regenerating the PIN, user can continue with retrying. User can be notified via email of failed attempts to print.
- If the user agrees to regenerate the PIN then the option will generate a random PIN and replace the old hash with the new hash generated using this random PIN.
- Also, regenerate option will send the random PIN to user registered email id/NFC/BLE authenticated mobile device. The user authentication and email/phone/NFC/BLE validation is beyond the scope of this paper.
- User will input the new random PIN delivered as PIN via email/phone number/NFC etc.
- Printer will generate hash from user input and compare it with the stored hash.
- If the hash matches then print job will succeed.

The below screen captures show the front panel view.

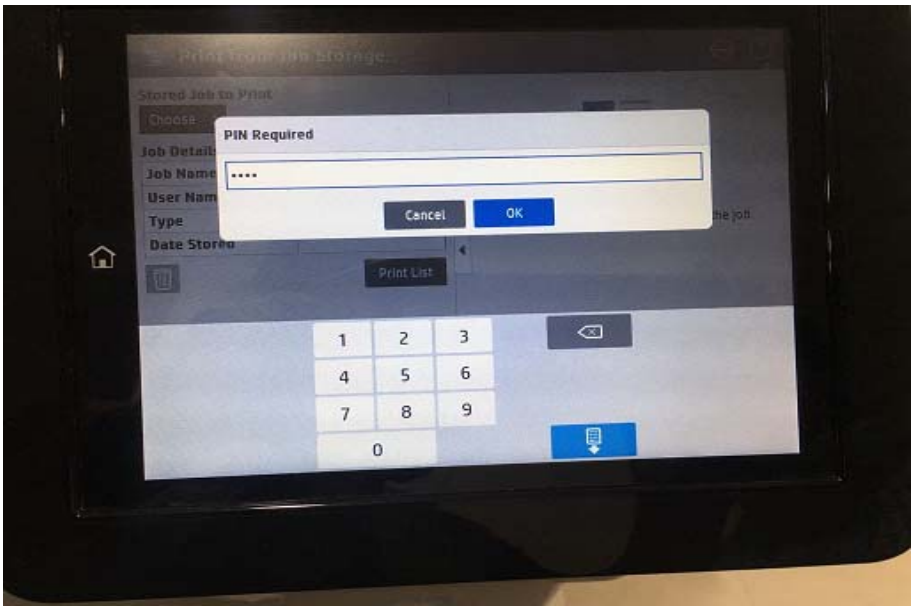


Figure 1: User attempting to PIN print

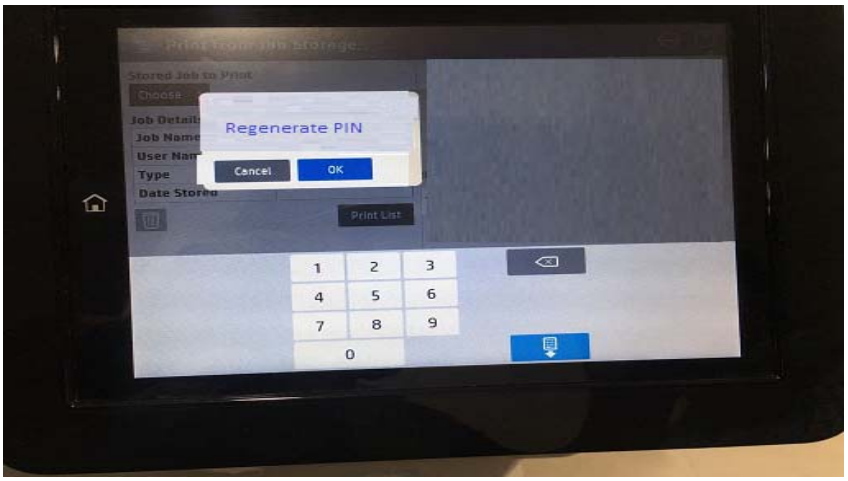
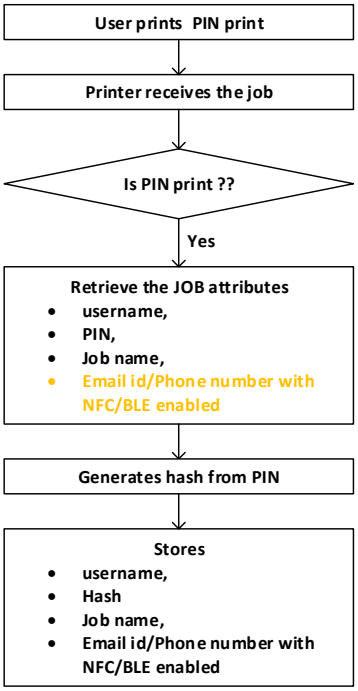


Figure 2: PIN Regeneration Option

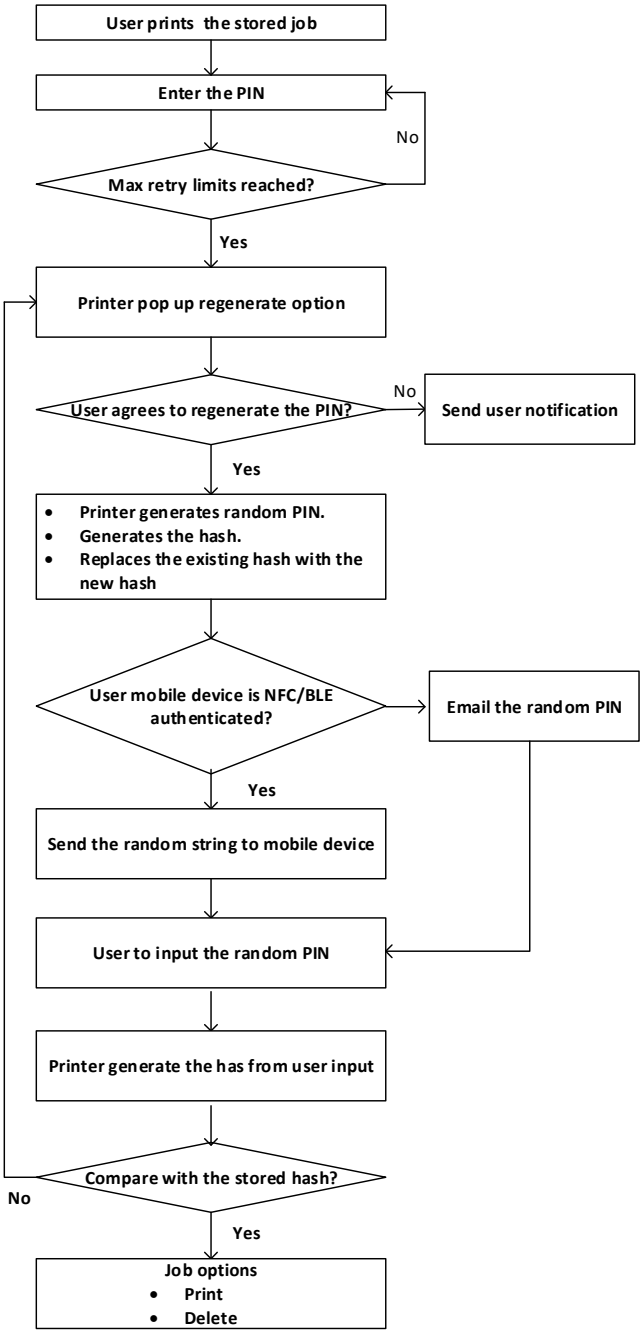
Figure 3: Printer transmitting Regenerated PIN via NFC/BLE.

Figure 4: Printer transmitting Regenerated PIN via E-mail.

Implementation Details



Printer generating hash from PIN print



User regenerating the PIN and print the job

Prior solutions and its disadvantages

There is no way to retrieve the PIN for the stored PIN prints. Also, the size of PIN is only four digits and the number of retries allowed is unlimited. This poses potential dictionary attacks.

Advantages

Improves the user experience by enabling the user to retrieve PIN any time. Eliminates the pain of performing factory reset for the permanent jobs. Enhances the data security at test by bringing down the chances of dictionary attacks.

The idea is to use the pre-authenticated device/email/phone associated with a user and use it for retrieving a print file secured with a PIN.

Disclosed by Manjunath Bhat Jayalakshmi, B N Divya, Rupam Banerjee Deb, V Lakshmi and Hiremath Poornima. HP Inc.