April 11, 2019

SECURE REMOTE WEBSCAN FROM UNAUTHORIZED WALKUP SCANS

HP INC

Secure Remote WebScan from Unauthorized Walkup Scans

Abstract

Remote WebScan is a feature which is increasingly used for digitization of physical data using Multi-Function Print Peripherals (MFPs) supporting a scanner bed. However, this brings forth potential security vulnerabilities such as when the walkup user is not identical to the remote web-scan client user; and hence could be a rogue user who maliciously might try to disseminate scanned data in conjunction with the legal remote scan.

Problem Statement

Existing Web-scan implementations don't prohibit a walkup user from roguely disseminating scanned data in parallel to sending it to the intended web-scan recipient. In fact, the problem is acute with two possible vulnerability scenarios viz.

a. Rogue user does illegal scan before legal remote web-scan
b. Rogue user does illegal scan after legal remote web-scan

Proposed Solution

Secure Remote Web Scan operations from unauthorized walkup scans

The idea proposes the following secure remote web-scan operational flow: -

1. A web-scan client user sends a web-scan request to the target MFP which then creates a skeletal scan job associated with the request.

2. Web-scan client user might then ask a walkup user to place the physical doc on the MFP's scanner bed to send the scanned image of it to web-scan client user using that skeletal scan job.

3. Now, the walkup user might intend to do a malicious scan operation such as printing the scanned document (Photocopy) either after or before doing the first legal remote web-scan. In either of these cases, a stored scan image of the of the walkup user's scan would be created on the MFP awaiting a PIN to be entered for processing further. This would not be a skeletal image but the actual digitized image of the document. Thus, all walkup scans are linked with a pin for full processing, till there is a pending skeletal remote web-scan job on the MFP.

4. These blocked walkup scans which are saved as stored scan jobs on the MFP, would be not processed further,
   a. till the MFP confirms with connected remote web-scan clients that its indeed not a duplicate/rogue scan of data which has been already remote web scanned This addresses the scenario where Rogue walkup user does illegal scan after legal remote web-scan.

      &&

   b. till all the pending remote web scan requests which were present at the time instant when the blocked scan job was initiated by the walkup user, are processed. - This addresses the scenario where Rogue walkup user does illegal scan before legal remote web-scan. For example, if there are 3 pending remote web-scan requests on the MFP when the blocked scan job was created, all the 3 need to be processed successfully to confirm that the blocked scan job was not an infringement of one of them.

5. Thus, if the walkup user selects the stored scan job request from the MFP's control panel, there are two scenarios to consider:

a) **If the selected stored scan job is empty**, a PIN is generated by the MFP and sent to the remote web-scan client device associated with the stored scan job. This is done to ensure the remote web-scan user is aware of the

exact time-instant when his stored remote web-scan job is getting processed by the walkup user. The walk-up user needs to enter that PIN and place the physical document on the scanner bed to release the scan job.

b) **If the selected scan job is non-empty**, the walk-up user needs to enter the PIN associated with the stored scan job request, which will be generated and sent to remote web-scan client matching the selected scan job (as explained in 9a below) or displayed on the printer front panel, if there are no matches.

6. After successful PIN authorization, scanned document will be sent to the remote web-scan client in scenario 5a or processed further as per the walkup user's choice in scenario 5b.

7. After successful processing of remote web-scan job, the scanner would also send a notification to the corresponding client requesting it to remain connected to it, till the client has assured itself that the physical document in possession with the walkup user has been secured. The processed remote web-scanned job would also be stored on the MFP, till the time the corresponding remote web-scan client is connected.

8. Once a new walkup scan request comes to the scanner, it will do a comparison of this new request with the scanned jobs that have already been remote web-scanned from the scanner/ MFP if their corresponding clients are still connected to the MFP.

9. Once all the previously scanned images are compared with the current scan image (using standard algorithms such as explained in References), there are two potential scenarios to consider when a walkup user tries to retrieve a blocked stored scan job:

   a) If the selected blocked scan image matches with any of the previously web-scanned images as discussed in step 7 above, the corresponding web-scan client would be notified by the MFP along with the PIN to approve/deny the requested blocked stored scan job from proceeding.

   b) If the current scan image doesn't match with any of the previously web-scanned images and all the pending remote web scan requests which were present at the time instant when the blocked scan job was initiated by the walkup user have been processed, a PIN is displayed for the walkup user on the MFP's front panel and the scan job is performed without notifying any of the connected remote scan users.

10. The Flowchart explains the above sequence of operations for retrieving a stored scan job.

Advantages

1. This solution ensures fool-proof security for a physical doc in hands of a walkup user from getting it wrongly disseminated using the MFP.
2. The beauty of the solution lies in the fact that it would work without any time constraints such as maintaining a big table of remote web scanned jobs for comparison.

References

[1] https://waset.org/publications/9998572/an-image-matching-method-for-digital-images-using-morphological-approach

Disclosed by Abhinav Yadav, Debayani Sarangi, .Sharanabasappa, Balaji Yalamarthi and Shakti Amarendra, HP Inc.

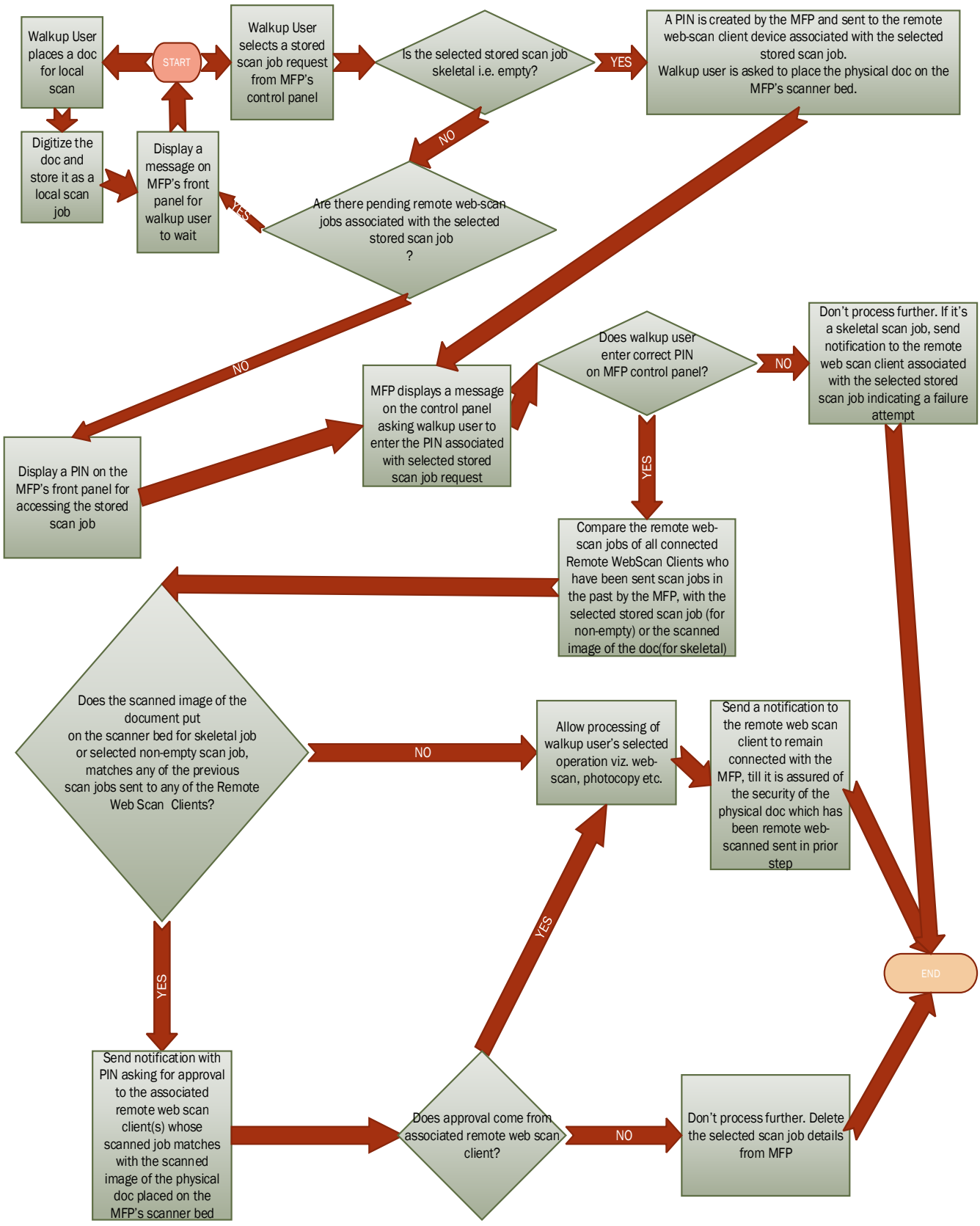

Figure 1: Operation flowchart of Securing Remote WebScan from unauthorized walkup scans