May 10, 2019

AUTHENTICATING WALKUP USER FOR SECURE REMOTE WEBSCAN

HP INC

Authenticating Walkup user for Secure Remote WebScan

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. After successful processing of each 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.

4. This happy path of remote scan job workflow would be affected adversely, if the walkup user intends 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, the walkup user is asked to disclose his identity which is confirmed with remote web-scan client user(s).

5. Thus, if the walkup user selects a scan operation (photocopy, san to email etc.) from the MFP's control panel, there are two scenarios to consider:

a) **<u>If there are pending remote scan jobs</u>** – In this case, suspicion could be that it's a rogue walkup user who has maliciously not chosen one of the pending remote scan jobs. The walkup user is then asked to share his/her digital photo with the printer via well-known techniques such as NFC/BLE to connect the walkup user's smartphone with the printer. For additional security, it might so happen that the MFP uses the digital camera available on the smartphone itself to click an instantaneous photo of the walkup user. The photo is then shared with the pending remote web-scan client users to confirm if they want to allow the walkup user to proceed with his/her intended scan operation.

b) **<u>If there are no pending remote scan jobs but remote web-scan clients are connected to the MFP</u>**- In this case, situation could be that the client has not yet assured itself that the physical document in possession with the walkup user has been secured. Hence, the walkup user would be asked to share his/her digital photo with the printer via the same steps as outlined in 5a above.

6. The Flowchart below explains the above sequence of operations for authenticating a walkup user.

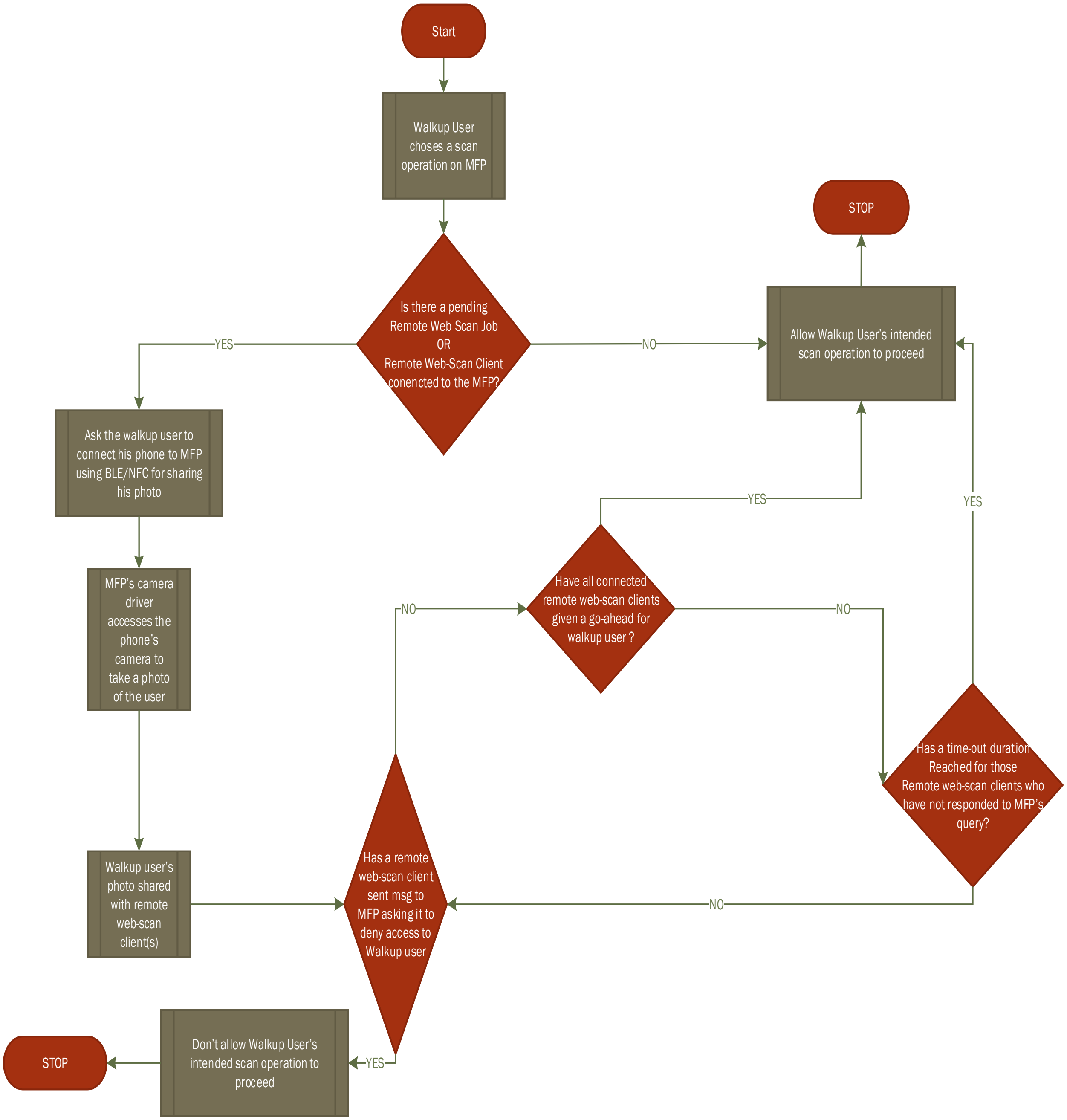
Start
Walkup User choses a scan operation on MFP
Is there a pending Remote Web Scan Job OR Remote Web-Scan Client conencted to the MFP?
YES
NO
STOP
Allow Walkup User's intended scan operation to proceed
Ask the walkup user to connect his phone to MFP using BLE/NFC for sharing his photo
YES
YES
MFP's camera driver accesses the phone's camera to take a photo of the user
NO
Have all connected remote web-scan clients given a go-ahead for walkup user ?
NO
Has a time-out duration Reached for those Remote web-scan clients who have not responded to MFP's query?
Walkup user's photo shared with remote web-scan client(s)
Has a remote web-scan client sent msg to MFP asking it to deny access to Walkup user
NO
STOP
Don't allow Walkup User's intended scan operation to proceed
YES

Figure 1: Operational flowchart of Authenticating Walkup User for Securing Remote WebScan from unauthorized walkup scans

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 doesn't need to store any scan jobs for comparison of walkup user's scan data with remote web-scanned data.

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