Technical Disclosure Commons

Defensive Publications Series

August 21, 2019

User account suggestions for access-restricted online resources

Christina L. Gilbert

Jonathan D. Hurwitz

Recommended Citation

Gilbert, Christina L. and Hurwitz, Jonathan D., "User account suggestions for access-restricted online resources", Technical Disclosure Commons, (August 21, 2019)
https://www.tdcommons.org/dpubs_series/2422

User account suggestions for access-restricted online resources

ABSTRACT

Mobile device users often have multiple account credentials, e.g., personal accounts, corporate accounts, etc., stored on their devices. A given webpage, document, or URL may be configured with permission for access via one user account but not for other user accounts. This disclosure describes techniques that automatically use or recommend credentials stored on a device to gain access to protected content.

KEYWORDS

- Document sharing
- Online sharing
- Protected content
- Access restriction
- Access control
- Credentials
- User account
- Account switching

BACKGROUND

Mobile device users often have multiple account credentials, e.g., personal accounts, corporate accounts, etc., stored on their devices. A given webpage, document, or URL may be configured with permission for access via one user account but not for other user accounts. A user is sometimes denied access from a device to an online resource due to the use of incorrect credentials even when correct credentials are stored on the same device. An access-restricted online resource, e.g., a shared document, a shared folder, etc. sometimes returns a message that advises the user to contact the owner of the web resource for permission to gain access. However, there is no automatic procedure to attempt access with all available user credentials.

DESCRIPTION

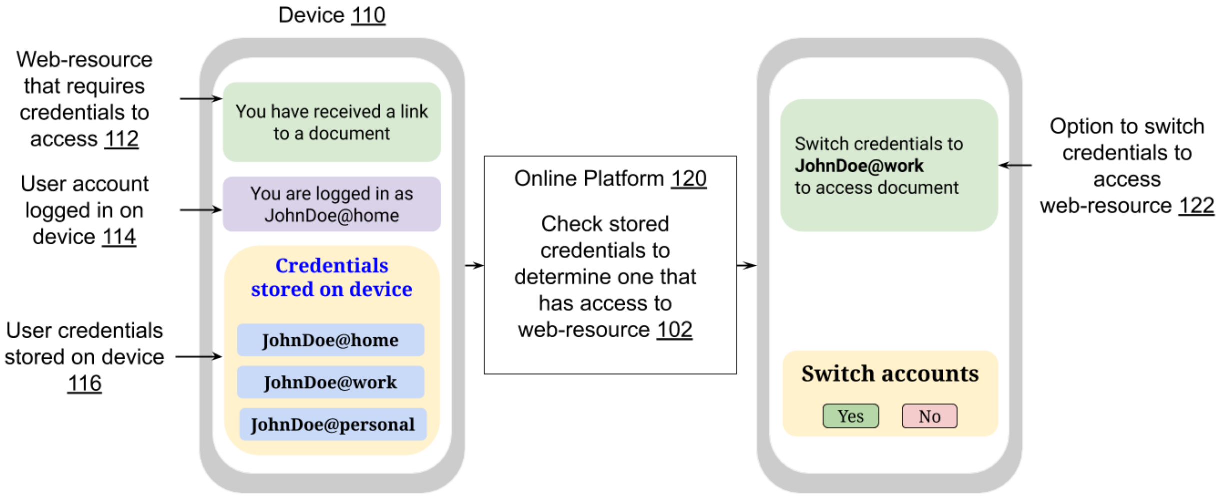
Device 110
Web-resource that requires credentials to access 112
User account logged in on device 114
User credentials stored on device 116
You have received a link to a document
You are logged in as JohnDoe@home
Credentials stored on device
JohnDoe@home
JohnDoe@work
JohnDoe@personal
Online Platform 120
Check stored credentials to determine one that has access to web-resource 102
Switch credentials to JohnDoe@work to access document
Option to switch credentials to access web-resource 122
Switch accounts
Yes
No

Fig. 1: Selecting the right credentials to gain access to a web-resource

Fig. 1 illustrates permissions-aware linking, e.g., selecting the right credentials from the different credentials stored on a device to gain access to a web resource, per techniques of this disclosure. The techniques described herein are implemented with user permission to access user credentials stored on the device.

As illustrated in Fig. 1, several different user credentials (116) are stored on a device (110). The user is currently logged in on the device with a first credential (114) and attempts to access a web resource with restricted access (112). Web resources can include, e.g., shared documents, spreadsheets, presentations, files, folders, images, videos, etc. With user permission, the available user credentials are provided to an online platform (120) that hosts the web resource. The platform automatically checks the credentials (102) to identify an available user credential that is permitted to access the access-restricted web resource.

If it is determined that the credential that provides access is not the one that the user is currently logged in with, an option is provided to the user (122) to switch credentials to access the web resource. If multiple credentials have access to the restricted content, the platform prioritizes the account that the user is currently logged in, or an account that was in most recent use.

Below are some example scenarios that illustrate the operation of the techniques.

Example 1: Account currently in use have access to restricted content.

The user is granted access using the in-use credentials.

Example 2: Account currently in use lack access to restricted content, but another logged-in account is permitted access.

The user is requested to switch credentials, using, e.g., a confirmation window, to access the web resource using the logged-in account.

Example 3: Account currently in use lack access to restricted content, but another logged-out account is permitted access.

The user is requested to switch to the currently logged-out account. The platform verifies the provided credentials to grant access. For security reasons, a logged-out account is selected only if specific criteria are fulfilled, e.g., if the account has been used on the device in the recent past, e.g., past two weeks.

Example 4: None of the stored accounts is permitted access to the web-resource.

The user is provided with an option to request access from the owner of the web-resource.

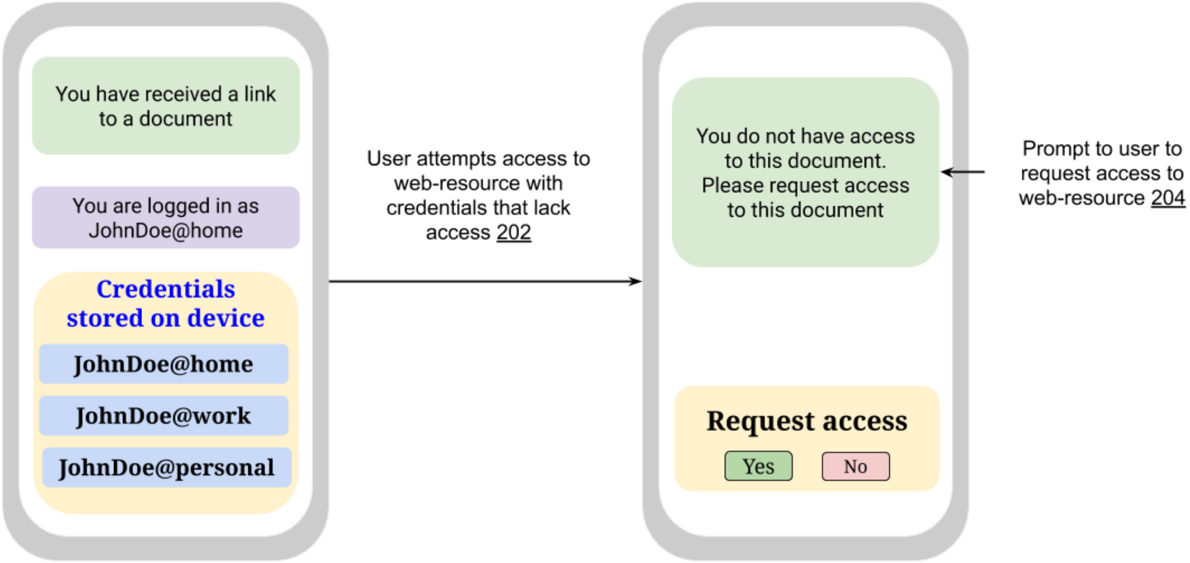
You have received a link to a document
You are logged in as JohnDoe@home
Credentials stored on device
JohnDoe@home
JohnDoe@work
JohnDoe@personal
User attempts access to web-resource with credentials that lack access 202
You do not have access to this document. Please request access to this document
Prompt to user to request access to web-resource 204
Request access
Yes
No

Fig. 2: Sequence of actions when no stored account is permitted access

This is illustrated in Fig. 2, where a user attempts access to a web resource with stored credentials for an account that is not permitted access to the resource(202). The platform that hosts the web-resource returns with a prompt to the user to request access to the web resource (204).

In this manner, the described techniques simplify access to access-restricted (protected) content by automatically selecting the correct credentials that grant access from available user accounts. Users can access protected web resources in a secure manner with just one click or touch, without need for manually determining the correct account and switching between user accounts, without the burden to remember the specific account that has access to the protected web-resource. The described techniques are implemented with user permission to access user data such as user names, passwords, or other information related to account credentials. The user can choose to turn off account suggestions. The techniques can help improve online document or file sharing services by automatically providing users access to shared items. Permissions-aware account switching can be implemented on any user device such as a computer, tablet, smartphone, wearable device, etc. that stores account credentials.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user’s social network, social actions or activities, profession, a user’s preferences, or a user’s current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user’s identity may be treated so that no personally identifiable information can be determined for the user, or a user’s geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

Mobile device users often have multiple account credentials, e.g., personal accounts, corporate accounts, etc., stored on their devices. A given webpage, document, or URL may be configured with permission for access via one user account but not for other user accounts. This disclosure describes techniques that automatically use or recommend credentials stored on a device to gain access to protected content.