Technical Disclosure Commons

Defensive Publications Series

August 30, 2018

Automatic Detection and Deletion of Unused Online Accounts

Emmanuel M. Arriaga

Automatic detection and deletion of unused online accounts

ABSTRACT

Users often create online accounts that are used only for a short period after which the user does not utilize the account anymore. Similarly, a user may stop using an account that was previously used regularly. The existence of such unused or stale accounts exposes the user to security and privacy risks, e.g., if the information held by the service providers of such accounts becomes available to third parties due to breaches, leaks, or sales. With user permission, the techniques of this disclosure detect unused or stale online accounts by detecting when a user does not login to an account for a long period, and facilitate deletion of the account.

KEYWORDS

- Unused account
- Stale account
- Dormant account
- Web login
- Password manager
- Account deletion
- Account tracking

BACKGROUND

Most online services such as email, social networking, file sharing, messaging, banking and payments, etc. require users to create an account with the service. Users often create online accounts that are used only for a short period after which the user does not utilize the account anymore. Similarly, a user may stop using an account that was previously used regularly, owing to reasons such as switching to another service, changing jobs, moving to another town, etc. If

such unused or stale accounts are not deleted, username and password information, as well as user data and metadata stored in these accounts continue to be stored by the service. Such data can expose the user to security and privacy risks, e.g., if the information becomes available to third parties due to breaches, leaks, or sales. Further, since many users reuse passwords and usernames across services, the exposure of information from one account can lead to the compromise of other accounts.

DESCRIPTION

The techniques of this disclosure, implemented with user permission, include detecting unused and stale online accounts by monitoring a database of account information and associated user login activity. If user does not log in to an account for a period exceeding a specified threshold value, the user is prompted to delete the account in order to protect the account information from being exploited. If the user decides to act on the prompt, the user is directed to log in to the account and follow steps for account deletion. If the user permits, account deletion can also be performed via automated mechanisms in cases where the online service provides such mechanisms, e.g., an Application Programming Interface (API) that permits account deletion.

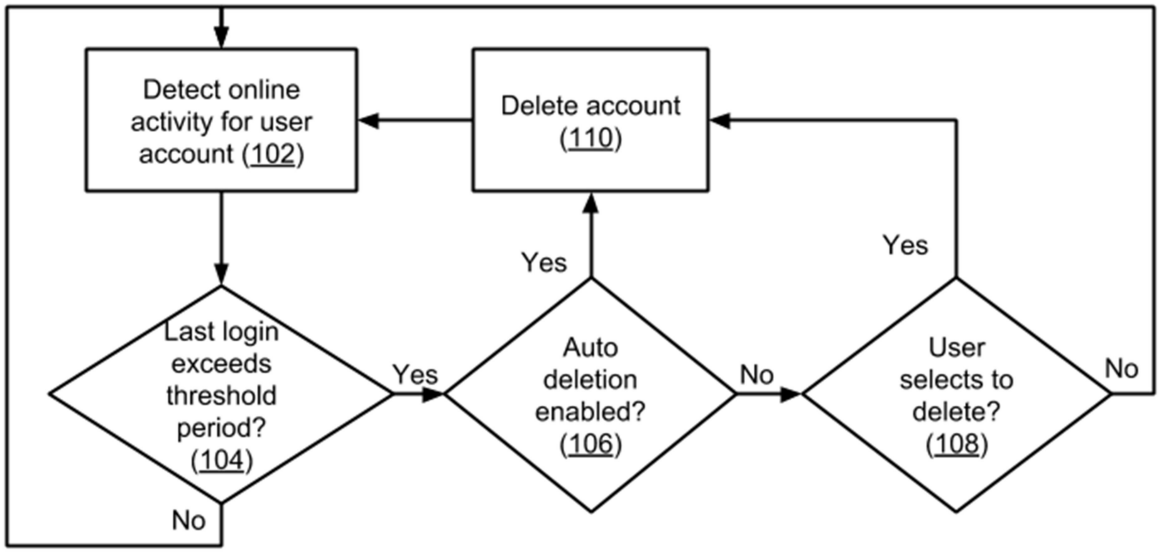

Fig. 1: Detecting unused and stale accounts for possible account deletion

Fig. 1 shows an implementation of the techniques of this disclosure. The techniques to recommend or automatically perform account deletion are implemented only upon user permission. The techniques can be implemented as part of a web browser application, a password manager application, an operating system, etc. or as a standalone application. Online activity for a user account for which the user has permitted access is detected (102). For example, the activity may be detected by accessing an online accounts database that includes information on various online accounts of the user and related activity. The database includes user-permitted information such as the web address of the account provider, username, account password, timestamp of last successful login, etc.

Based on the detection, it is determined whether the last successful login for a user account in the database occurred more than a threshold period of time ago, e.g., more than six months ago, more than a year ago, etc. (104). The threshold period may be user-specified or determined automatically. If the last login occurred at a time that exceeds threshold period, it is determined whether the user has enabled auto deletion of inactive accounts (106). If the user has

enabled auto deletion, the online account is deleted from the service (110). If the user has not enabled auto deletion, a prompt is provided to the user indicating that the account is inactive (108). If the user selects to delete, the online account is deleted from the service (110).

Account deletion may include having the user log in to the inactive account, and following manual steps to delete the account. Alternatively, if the user enables auto deletion, the account may be automatically deleted using relevant automated account deletion capabilities via an API provided by the service that hosts the account.

If the user decides not to delete the account, the accounts database is updated to include the decision such that the user is not prompted again immediately to delete the account. For instance, a flag may be set in the database indicating that the user opted to not delete the account upon previous prompt or the timestamp for the last successful login may be set to the timestamp of the user decision in response to the prompt, thus ensuring that the next deletion prompt does not occur until the specified period threshold has passed again.

The frequency at which an account is examined to determine whether it is an unused or stale account, and the threshold period beyond which an account is considered to be unused can be specified by the software that implements the techniques, or by the user. The frequency and the threshold may vary across accounts or account types, such as email account, financial account, social media account, etc. Additionally, if the online service permits account deletion via automated mechanisms, the user may permit automatically deleting the account after a specified period. Such permission may be granted at the time or account creation or any time thereafter.

With user permission, the techniques of this disclosure can include mechanisms that utilize knowledge of the user's typical online activities in order to predict if an account is likely

to be used much longer beyond the time of its creation. If an account indicates a sufficiently high probability of short-term use, the user may be prompted for a decision regarding account deletion. Alternatively, if the user permits, such accounts may be automatically flagged for deletion. Similarly, with user permission, the techniques of this disclosure may be applied to predict which online accounts are likely to be affected by changes in the user's context, such as a move or a job switch.

In situations in which certain implementations discussed herein may collect or use personal information about users (e.g., user data, information about a user's social network, user's location and time at the location, user's biometric information, user's activities and demographic information), users are provided with one or more opportunities to control whether information is collected, whether the personal information is stored, whether the personal information is used, and how the information is collected about the user, stored and used. That is, the systems and methods discussed herein collect, store and/or use user personal information specifically upon receiving explicit authorization from the relevant users to do so.

For example, a user is provided with control over whether programs or features collect user information about that particular user or other users relevant to the program or feature. Each user for which personal information is to be collected is presented with one or more options to allow control over the information collection relevant to that user, to provide permission or authorization as to whether the information is collected and as to which portions of the information are to be collected. For example, users can be provided with one or more such control options over a communication network. 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. As one example, a user's identity may be treated so that no personally identifiable information can

be determined. As another example, a user's geographic location may be generalized to a larger region so that the user's particular location cannot be determined.

CONCLUSION

The techniques of this disclosure involve detecting unused and stale online accounts by accessing, with user permission, a database of account information and associated user login activity. If a user does not login to an account for a period exceeding a specified threshold value, the user is prompted to delete the account. If the user permits, account deletion is performed via automated mechanisms. The implementation of the techniques described above can be provided as a standalone application or integrated within a web browser, a password manager, an operating system, etc. or implemented as a combination of these two approaches. Deletion of unused or stale accounts in this manner reduces security and privacy risks to the user.

REFERENCES

- Fredinburg, Dan, Keith Patrick Enright, and Andrew Swerdlow. "Zombie detector and handler mechanism for accounts, apps, and hardware devices." U.S. Patent 9,280,592, issued March 8, 2016.
- https://justdeleteme.xyz/