Technical Disclosure Commons

Defensive Publications Series

September 10, 2018

Context-Based Permissions to Control Access to Data

Steffen Meschkat

Context-based permissions to control access to data

ABSTRACT

Users commonly provide permissions to software applications running on their personal computing devices to access data stored on their devices. Context-based permissions and controls are described that enable users to directly make decisions about data access by software applications in the context of ongoing user activity. The user context and permissions are persistent, and applied to other devices of the user.

Data that are produced by various services are packaged into entities, and access is granted or denied to applications one entity at a time, rather than to a service that generates the data entities. With user permission, a record of past user activities is maintained by the operating system. The record is made available for inspection by the user and utilized as a template for future permissions. Past interactions are utilized, and interpretation or corrective action is performed upon permission from the user. For ease of interaction, such permission may be obtained, e.g., at initial setup, and is modifiable.

KEYWORDS

- Permission
- User experience
- Data access
- Permission granularity
- Container
- Operating system

BACKGROUND

Users commonly provide permissions to software applications running on their personal computing devices to access various units of data stored on their devices. The permissions involve decisions regarding the units of data and their association with respective software applications. A device connected to the internet has ready access to new software applications throughout its useful life. Devices that include sensors such as cameras and microphones continually generate new units of data. Consequently, the permissions cannot always be provided at a time of manufacture of a device and decisions about permissions are made continually during its use.

Commonly, these decisions are not made directly by a user of the device. Instead, the user establishes or influences policy, which is then invoked to automatically make a decision when needed. The policy typically relies on an architectural principle that a particular software application can automatically access data that was created by the software application. In addition, a catalog of decisions regarding the system provided services accessible to the software application is provided by the user when the software application is installed or first executed.

Policy based decisions provide an advantage in that the policy can be complex and dynamic, and that it can be partially or fully delegated (for example, to an App store or to a corporate IT department). Additionally, the user does not have to be consulted for every decision, which could be burdensome to the user when using software applications that process large numbers of units of data at a time.

However, policy-based decisions are often opaque to the user with regard to privacy. An individual user does not have ready access to information about the purpose, duration and conditions of access that specific software applications have to specific units of data.

DESCRIPTION

This disclosure describes context-based permissions and controls for computing devices. The context-based permissions and controls enable users to directly make decisions about data access by software applications without having to make repeated decisions.

Per techniques of this disclosure, decisions about data access by software applications are taken by users in context of ongoing user activity. Computing devices that implement the described techniques, e.g., as part of an operating system, store application data in generic units or chunks, referred to as "entities." Software applications are executed within containers and are connected to the entities.

The operating system launches applications with entities to operate upon analogous to the manner in which applications are utilized to access and edit files in traditional operating systems. User input is interpreted as the specification of an entity to be provided to an application. User permission is provided for software applications to access specific entities, based on the user activity context.

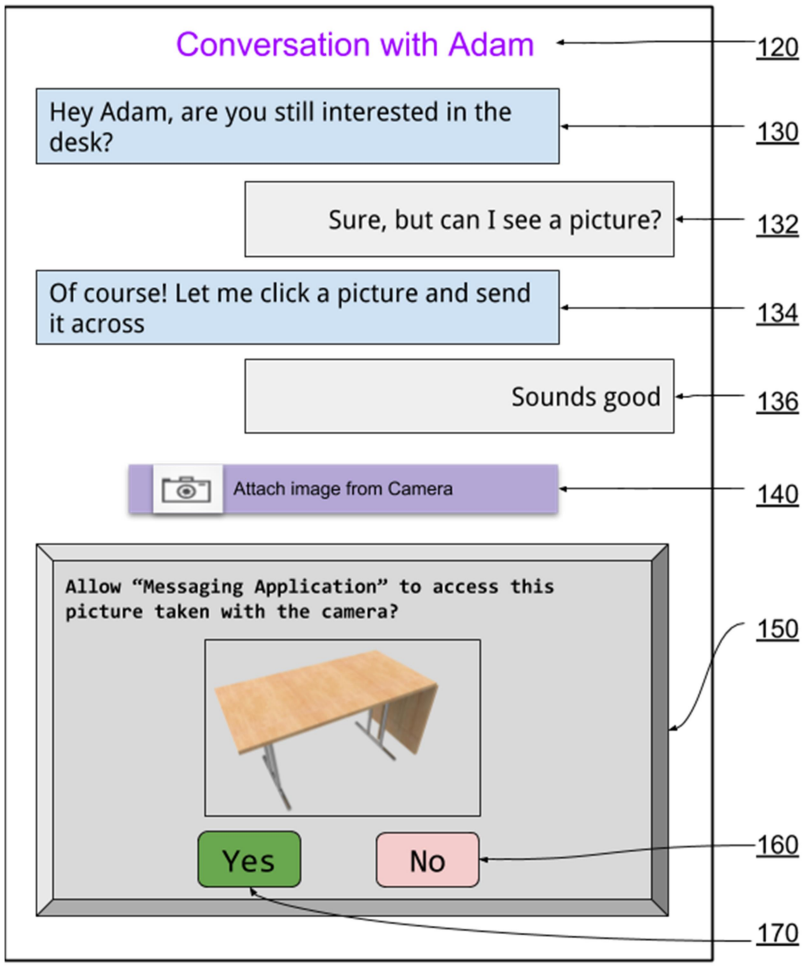

Fig. 1: Granting permissions on the basis of context and the data requested

Fig. 1 illustrates user permission being granted to a software application to access an entity in an example conversation (120) conducted using a messaging application. After an exchange of messages (130-136), the user attempts to attach (140) a picture taken with the camera (150) of a user device. The user can choose to either grant (170) or deny (160) permission for the messaging application to access the entity (data unit) that represents the picture taken by the camera.

Once the camera service generates the picture, the access permission for the messaging application remains associated with that picture for the duration of the user activity, but no permission is implied for other pictures taken by the camera service at a future time.

The user context and permissions are persistent, and are applied by the device at a later point in time and on other devices operated by the user. For example, in the scenario illustrated earlier, the user permission provided to the messaging application for the context of this conversation can automatically be applied on a second device of the user, e.g., for resuming the same messaging conversation by adding another party and sending the same picture to the added party.

Data that are produced by various services (camera, sensors, etc.) are packaged into entities such that access can be given or denied to applications one entity at a time, rather than to a service that generates the data entities. A record of past user activities is maintained by the operating system and is inspectable by the user. The record is utilized as templates for future permissions. Access permissions for programs associated with prior activities can be restored by the user to data associated with the previous activities, according to previously granted permissions.

Per techniques of this disclosure, user permission for an application to access data entities is provided on the basis of user activity context and relationships with individual data entities. Consequently, an application that is provided access to a specific data entity in a particular user context is not automatically provided access to the same data entity in a different user context, and is not automatically provided access to other data entities generated by the service that generated the particular data entity.

With user permission, a historical record of permissions provided to various applications to entities is maintained that is accessible to the user. Previously granted permissions remain active in the record for resumption by the user. A user interface enables users to grant permissions for routine operations, e.g., typically at an initialization stage of the operations.

The historical record is utilized to enable users to make decisions and provide permission for new user activity contents. The user interface assists the user, for example, by providing suggestions and recommendations for software applications to use with certain data entities, as well as providing suggestions and recommendations for suitable permissions to provide to software applications.

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

Context-based permissions and controls are described that enable users to directly make decisions about data access by software applications in the context of ongoing user activity. The user context and permissions are persistent, and applied to other devices of the user. Data that are produced by various services are packaged into entities, and access is granted or denied to applications one entity at a time, rather than to a service that generates the data entities. With user permission, a record of past user activities is maintained by the operating system. The record is made available for inspection by the user and utilized as a template for future permissions. Past interactions are utilized, and interpretation or corrective action is performed upon permission from the user.