Technical Disclosure Commons

Defensive Publications Series

January 18, 2019

Controlling access by tagging data

Juan Vasquez

Jesper Johansson

Controlling access by tagging data

ABSTRACT

A customer (first party) uses an application developed by an application service provider (second party). A third party needs legitimate access to data of the customer stored on a server operated by the application service provider. In such a scenario, the third party requests the customer to permit the third party to access to such data. However, in some instances, the type of access requested by the third party is broad. This disclosure describes techniques to restrict the types of data that are made available to the third party by enabling a customer to tag data stored by the provider. Further, the customer can specify rules that govern sharing of tagged data with the third party.

KEYWORDS

- permission
- authorization
- secure data access
- OAuth

BACKGROUND

There are several contexts in which users delegate tasks to other users and/or utilize software or services provided by various other parties. In these situations, the delegate user or the service provider needs to be able to access some user data of the delegating user.

For example, a user that is a business executive utilizes an online e-mail service provider that maintains an e-mail account for the business executive. Further, the business executive employs an executive assistant. To perform job functions, the executive assistant

needs to be able to access the executive's emails and have the ability to respond on behalf of the executive, e.g., to customers, business associates, etc.

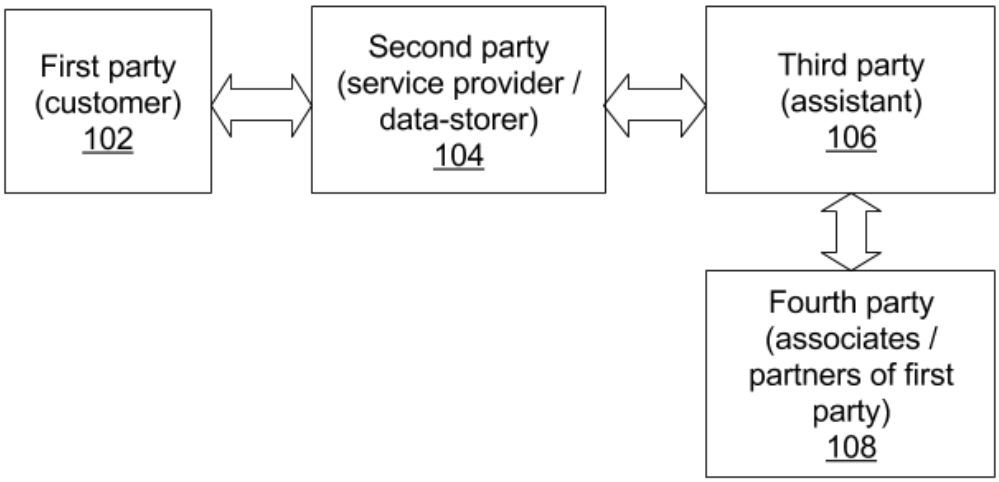

Fig. 1: Data-sharing between various parties

Fig. 1 shows a standard model by which data is shared among various parties. A first party, a customer (102), uses an application and generates data within the application. Such data belongs to the customer and is stored on a server belonging a second party, the application service provider (104), with consent of the customer. A third party, e.g., an executive assistant (106), needs legitimate access to data that belongs to the first party and is stored by the second party. The third party requests the first party, e.g., via the application, for permission to access such data. Upon receipt of permission, if granted, the third party can use such data, e.g., to interact with a fourth party (108) on behalf of the first party, under terms established by the first party. The fourth party may be, for example, associates or partners of the first party. The model of Fig. 1 is commonly used in many online systems, and is illustrated with the example below. The model also applies to the examples (executive assistant, price-drop monitoring application) described above.

Example: The first party (102) is an e-commerce vendor. The second party (104) is a data storage / warehousing / email service provider used by the first party. The fourth party (108) is a customer of the first party. The third party (106) is an external vendor or contractor of the first party tasked with managing the first party's e-commerce offerings, monitoring the first party's emails, and responding, for selected topics, to the fourth party on behalf of the first party.

There are a variety of options that the first party can utilize to provide data access to the third party. A delegation system uses Open Authorization (OAuth) tokens to provide the third party access to first-party data stored with the second party. The OAuth scope requested of the first party by the third party typically includes one or more of the following:

- Viewing the first party's profile information,
- Access email addresses of the first party,
- Read, send, modify, and/or delete emails of the first party, etc.

DESCRIPTION

An application service provider, e.g., an email provider, typically offers application programming interfaces (APIs) that allow a user to call particular services provided by the service provider. In the context of an API, the user creates a label that is automatically applied to data associated with the API. When a third party asks for access to data of the first party, e.g., through an OAuth request, only labeled data is provided.

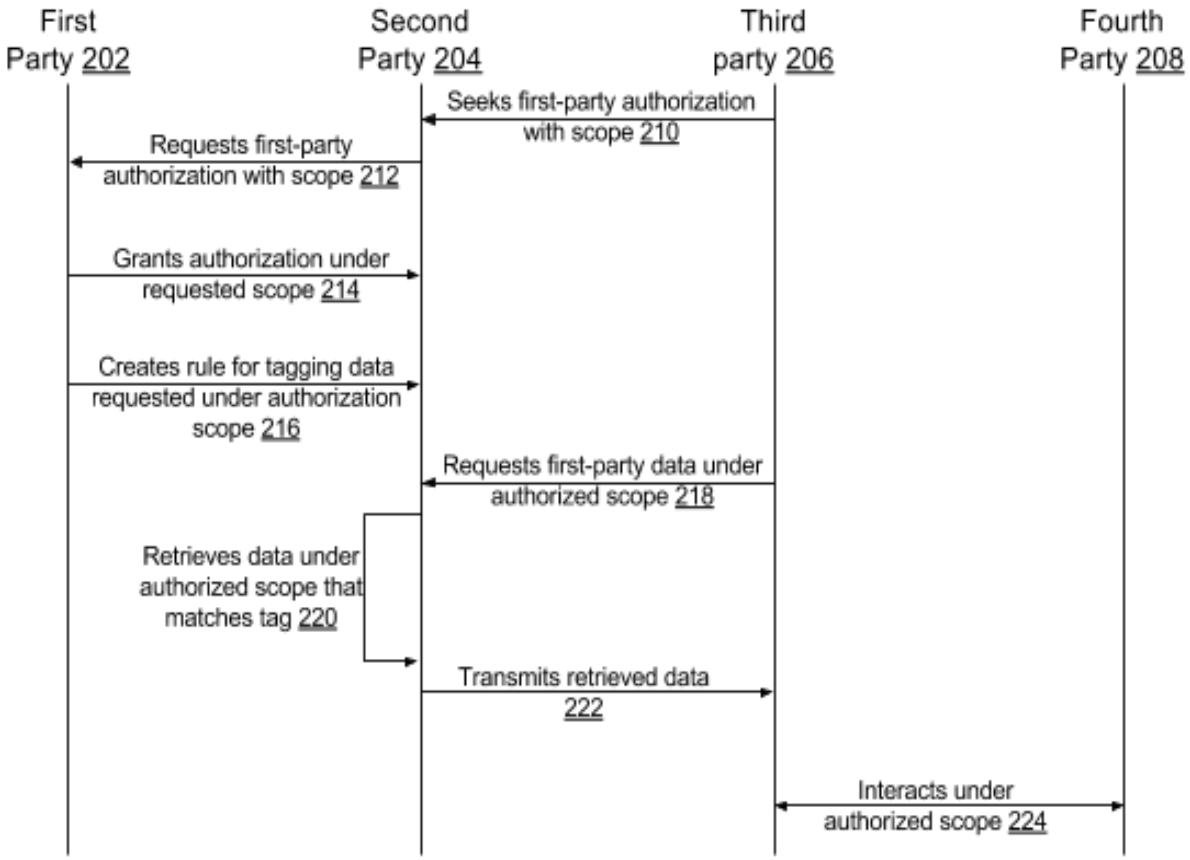

Fig. 2: Granting a third party controlled access to data

Fig. 2 illustrates a process to successfully grant to a third party controlled access to data that belongs to a first party. A third party (206) seeks from a second party (204) authorization with a specific scope (210) for data owned by a first party (202) that is stored with the second party. The second party forwards the data-access request to the first party (212). The first party grants authorization under the requested scope (214). The first party also creates rules (216) for tagging data that is requested under authorized scope.

The third party requests (218) from the second party, under the now-granted authorized scope, data belonging to the first party that is stored with the second party. The second party retrieves data (220) under authorized scope that matches the tag created by the first party. The

second party provides the retrieved data to the third party (222). The third party uses this data to interact under authorized scope (224) with a fourth party.

Example: Restricted access to email account

A customer (first party) uses an email service provided by an email service provider (second party). The customer interacts via email with an e-commerce site "eComm.com" (fourth party). The customer uses a price-monitoring service (third party) to check for reductions in prices of items recently purchased from the e-commerce site. The customer defines a rule that applies the tag "eCommOrderConf" to incoming email from eComm.com that contains the string "Order Confirmation."

When the price-monitoring requests access to the customer's email, e.g., under previously granted OAuth scope, such access is granted only to emails that bear the tag "eCommOrderConf". In this manner, the monitoring service is provided access to specific emails that are necessary for its services, while access to other content of the customer's email account is denied. Further, sent messages also get that tag if they were created through use of the same scope.

Example: Managed delegation of email account

A business executive (first party) authorizes an executive assistant (third party) to transmit email on their behalf. The executive wishes to restrict email transmittals. In this case, the business executive creates authorization scope that allows the executive assistant to compose emails but not send those via the business executive's email account. The emails require approval by the business executive prior to transmittal.

Another way to control email transmittal by the executive assistant is to include additional configuration controls to determine recipients to whom the executive assistant can

send mail under the granted scope. For example, under the tag “eCommOrderConf”, such email transmittals can be limited to customerservice@eComm.com. A request by the executive assistant to send email to other recipients is automatically denied. If the tag does not exist, or there is no email with that tag, the email service provider (second party) simply sends a blank response to the executive assistant. If the scope has not been granted, then the email service provider responds with an access-denied error.

In this manner, the permission scope is made dynamic based on user-defined labels. The label acts as an OAuth sub-scope. This extends the OAuth standard, without need to modify the standard itself. However, it is possible to achieve similar results by extending the OAuth standard. In order to do so, a metadata attribute for labels or sub-labels is added. Extending the standard thus is possibly more flexible for software developers, as no modifications are necessary to the URL associated with the scope. Instead, compliant software applications can submit the label information separately. Requests can also be composed without knowledge of the full scope, as the scope remains identical for every user, as opposed to user-defined scope.

A second party that hosts data belonging to a first party can create rules for the first party, thereby offering for the first party pre-created rules to choose from. A second party can also provide an API for a third party to enable the first party to choose from pre-created rules. Such an API can use OAuth but with a temporary scope.

Techniques described herein are applicable for a variety of cloud-based services, e.g., online document creation, sharing and management; web-based e-mail, calendar and other business applications; web-based financial applications; e-commerce; social media; etc.

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, user's online history 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

This disclosure describes techniques to control access to data belonging to a first party (e.g., a customer) that is stored at a second party (e.g., application server provider) and for which access is requested by a third party (e.g., another application). The techniques effectively

establish a sub-scope within an existing authorization scope such that only data that is labeled in a manner specified by the first party can be shared with the third party.