July 03, 2017

On-Demand Security Token Linking

John D. Lanza
Foley & Lardner LLP

ON-DEMAND SECURITY TOKEN LINKING

DETAILED DESCRIPTION

When interacting with a virtual personal assistant, such as Google Assistant, a user may request a specific service or action to be performed by the virtual personal assistant. The service or action can include, for example, a ride service by a specific provider, an online streaming service, or accessing an online resource (e.g., via a corresponding URL). Also, the virtual personal assistant may propose an alternative service to the user responsive to the user's request. Executing the user's request or accessing the alternative service may involve secure access steps such as user authenticating with a service provider, requesting access authorization to an online resource from another entity, or granting access to an online resource to another entity. In some instances where a user account for the requested (or alternative) service does not exist, the secure access steps may further include creating a user account. The virtual personal assistant may identify and automatically perform, responsive to the user's request, the secure access steps to link a user's client computing device to the requested (or alternative) service or perform the user requested actions.

By automatically executing secure access steps required to link the user to a service or perform a user-requested action, a data processing system hosting the virtual personal assistant can improve user experience and reduce the back and forth communications between the data processing and the client computing device. For example, getting back to the user each time a secure access step is identified can increase the amount and frequency of communications between the data processing system and the client computing device. Also, reverting back to the user and/or requesting the user to interfere and manually perform the secure access steps can

irritate the user and undermine the need for or role of virtual personal assistants. Systems and methods described herein allow for the data processing system automatically creating user accounts, requesting access to online resources, granting access to another entity, or executing other secure access processes responsive to a user request for a service or online action.

The data processing system can, for example, facilitate creation of user accounts associated with the user in a database of a service provider device such that the service provider device can communicate with, and provide requested services to, the client computing device. Also, the data processing system can identify that the user does not have access authorization to a requested online resource, and send a request for access authorization to an entity managing the online resource. The data processing system may also identify when generating a communication for sending to another entity that the intended recipient does not have access authorization to an online resource associated with a URL in the generated communication. In response, the data processing system can take proper actions to grant the intended recipient access authorization to the online resource.

FIG. 1 is an illustration of an example method 100 for automatically executing secure access tasks associated with a requested online service or online action. The method 100 can be performed by client computing device and a data processing system communicatively coupled to client computing device. The method 100 can include receiving an input speech signal indicative of a request or command made by a user of a client computing device (step 105). The client computing device can receive the input speech signal via a respective microphone. The user can initiate a conversation with an instance of a virtual personal assistant executing one the client computing device and/or the data processing system. For instance, the client computing device can include an executable script or program (e.g., a front-end module of the virtual

personal assistant) executed to control input and output speech signals associated with the virtual personal assistant, and the data processing system can include back-end modules of the virtual personal assistant for processing input speech signals, executing tasks and commands associated with received input speech signals, generating output speech signals, maintaining states of conversations with the user of the client computing device, or a combination thereof.

During the conversation, the user can request an online service, such as scheduling or setting a ride with the provider Uber (or other provider). The virtual personal assistant may suggest or propose an alternative provider of the requested service. For example, the virtual personal assistant may propose a ride with the provider Lift instead of Uber. The user may request access to an online live streaming service, such as a live streaming session of a sports game. The user may request the virtual personal assistant to read an email message (or other type of message) received from another entity. The message can include a link (e.g., URL) to an online document (e.g., a Google Docs document, a Google Sheets document, or the like). The user may follow up during the conversation with the virtual personal assistant to request access of the online documents associated with the link in the message. The use may request the virtual personal assistant to draft an email message (or other type of message) that includes a URL of an online document associated with the user.

The input speech signal can be indicative of a request of an online service (e.g., live streaming), a confirmation to proceed with an alternative service (e.g., a ride with Lift instead of Uber), request to read a message or access a link therein, a request to draft a message or insert a link therein, or the like. The font-end module of the virtual personal assistant may include a natural language processor component for processing speech signals such as the received input signal. Alternatively, the client computing device may transmit the received speech signal to the

data processing system for processing by a natural language processor component of the data processing system.

At step 110, the method 100 can include the data processing system (or the client computing device) identifying, by processing the input speech signal, a service or online action requested by the user of the client computing device. The natural language processor component can machine-translate the speech signal into a corresponding text signal. If the machine translation is performed at the client computing device, the client computing device can transmit the generated text signal to the data processing system. The data processing can parse the text signal to identify one or more trigger keywords defining a specific request or command by the user of the client computing device. For example, keywords like “live stream of,” “ride,” read email from,” write email to” or keywords indicative of the service provider name such as “Uber,” “Lift”, or “YouTube,” can be indicative of the service or online action requested by the user of the client computing device. The data processing system can determine the online service or online action requested by the user based on the identified keywords associated with the received input speech signal.

At step 115, the method 100 can include the data processing system identifying one or more secure access tasks associated with the requested online service or requested online action. For example, if the keywords associated with the input speech signal indicate a request for a service from a given provider (e.g., scheduling a ride with Lift or playing a live stream from livestream.com), the data processing system can access a database (or a webpage) of the service provider to request the service for the user, and in response receive an indication of (or request for) user account authentication from a device of the service provider. For instance, the device of the service provider may provide a login webpage to the data processing system. The data

processing system can determine based on the received login webpage that user account authentication is needed in order to link the requested service to user of the client computing device.

The keywords associated with the input speech signal can be indicative of a command to read a specific email message or list recently received email messages. The data processing system can scan the email message(s) and identify a link embedded therein. The data processing system can identify that accessing the online resource (e.g., online document) referenced by the link requires an access authorization from an entity managing the online resource. The data processing system may activate the link and receive a message indicative that the user is not authorized to access the resource associated with the link. Responsive to the received message, the data processing system can deduce that access authorization is required.

The keywords associated with the input speech signal can be indicative of a command to draft an email message (or other type of message) and/or to insert a link of an online resource or document associated with the user in the drafted message. The data processing system can access a database associated with the user and determine that the online resource is associated with an access policy set by the user. For example, the access policy may restrict access to the online resource to a specified list of users (or entities). The data processing system may determine that the intended recipient of the drafted message is not in the specified list of users. In response, the data processing system can deduce that access authorization for the online resource needs to be granted to the intended recipient of the drafted email message.

At step 120, the method 100 can include the data processing system performing the one or more identified secure access tasks associated with the online service or online action. For instance, if the data processing determines that a user account authentication is needed, the data

processing system can first determine whether an account with the service provider of the user (or the respective client computing device) exists. The data processing system may check a database (or a data structure) associated with the user or the client computing device to determine whether a user account for the service exists. If a user account exists, the data processing system can use corresponding authentication credentials (e.g., login and password) to access resources of the service provider (or a device of the service provider).

If no user account exists for the requested service, the data processing system can create an account for the user at a database associated with the service provider or a device thereof. The data processing may access a database of the user to retrieve user information (e.g., user name, email address, home address, date of birth, device ID, device IP address, etc.) needed to create the account. The database may include security policies (e.g. assigned by the user) associated with various pieces of the user's personal information. For example, the user's personal information may include various email addresses associated with different security policies. The security policies may indicate that a given email address is not to be used without the user's approval or that some information has to be encrypted or masked before being delivered to service providers. The data processing system can retrieve user information from the database according to the security policies. The data processing system may generate (e.g., using a random string generator) a password for the account to be created. The data processing system can then provide the user information to the service provider device to generate the user account.

If the data processing system determines that access authorization is required to access an online resource associated with a link in a received email message, the data processing system can send a request to the entity managing the online resource for access authorization. Sending

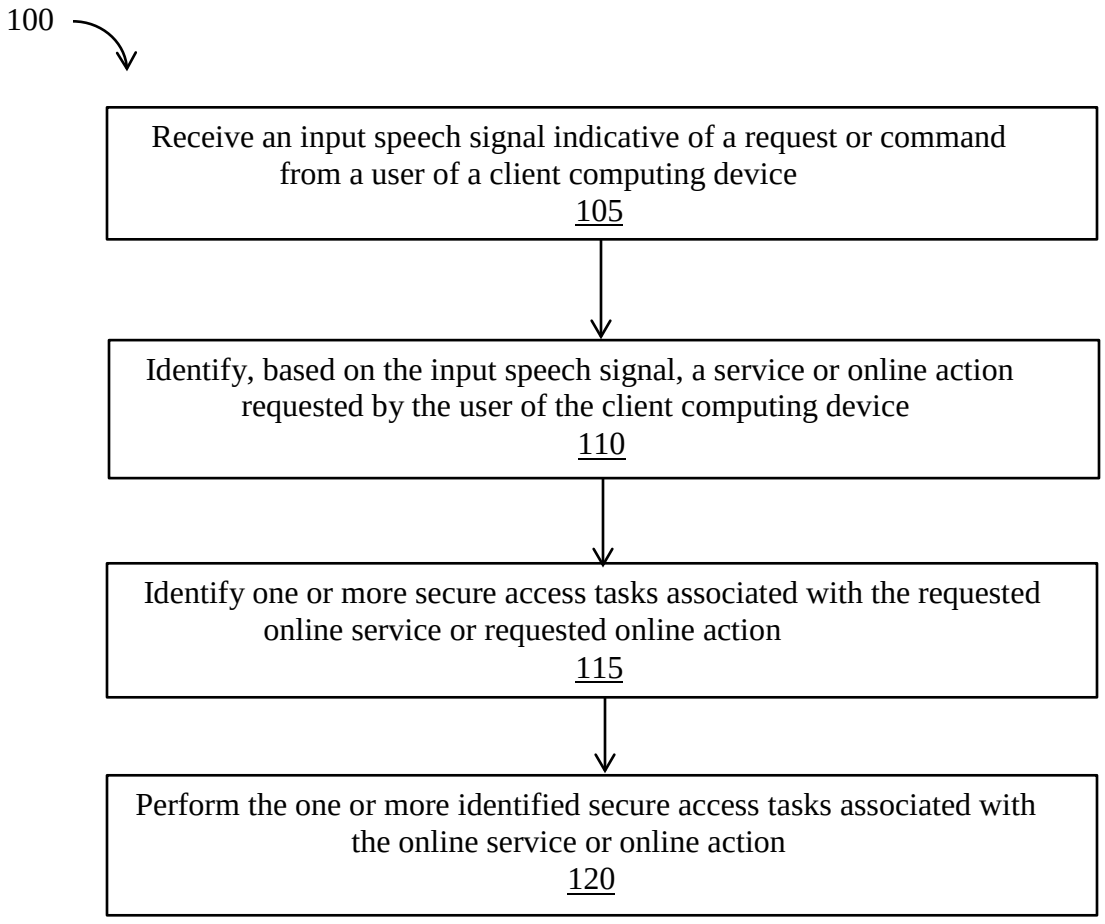
the access authorization request can include actuating an interactive icon or link received responsive to actuating the link referencing the online resource. The data processing system may monitor an email inbox of the user to detect receipt of an email message indicating grant of access authorization to the user.

If the data processing system determines that access authorization for the online resource in the drafted email message needs to be granted to the intended recipient of the drafted email message, the data processing system can access a database or a data structure associated with the user to assign access rights to the intended recipient of the drafted email message. The data processing system may use the intended recipient's email address to assign the access rights.

At step 125, the method 100 can include the data processing system performing the requested online service or online action. For instance, once the user account for a requested service is created, the data processing system can communicate with a device of the service provider to link the requested service to the client computing device of the user. For example, if the requested service is live streaming, the data processing system can cause a live streaming session between the service provider device the client computing device to be initiated. If the requested service is scheduling a ride, the date processing system can schedule the ride on a database or device of the service provider and provide a confirmation (e.g., audio confirmation) to the user via the user's client computing device. In the case of a command to compose an email message, the data processing system can insert the link of the online resource associated with the user in the email message and/or send the email message once access rights are granted to the intended recipient. In the case of a command to read or check for an email message, the data processing system may display, on the user's client computing device, the resource

referenced by the link in the received email message once a confirmation of granting access rights to the user are received.

The automatic execution by a virtual personal assistant of secure access tasks associated with a requested online service or online action, as described above, can improve user experience and reduce the number of communications between the virtual personal assistant and the client computing device in a given conversation. The examples of secure access tasks described above are not limiting and other tasks can be executed by the virtual personal assistant depending, for example, on the type of service or online action requested.



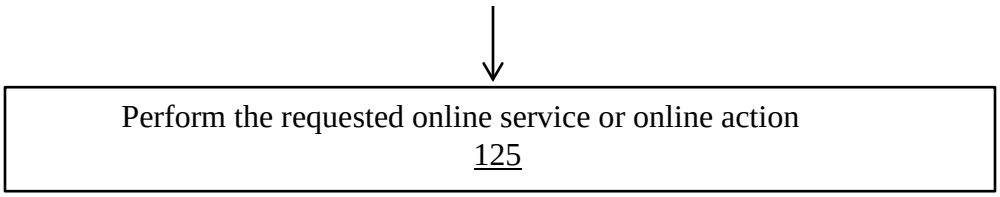


FIG. 1

ABSTRACT

Systems and methods described herein allow for automatic execution by a virtual personal assistant of secure access tasks, such as user account authentication or acquiring/granting access authorization, associated with an online service or online action requested by a user of a client computing device. The client computing device can receive an input speech signal indicative of a request or command from a user of a client computing device. A data processing system communicatively coupled to the client computing device can identify, based on the input speech signal, a service or online action requested by the user of the client computing device. The data processing system can identify one or more secure access tasks associated with the requested online service or requested online action. The data processing system can perform the one or more identified secure access tasks associated with the online service or online action. The data processing system can then perform the requested online service or online action.