September 29, 2017

USING AN INTERACTIVE ASSISTANT AS A PASSWORD VAULT

Google Inc.

USING AN INTERACTIVE ASSISTANT AS A PASSWORD VAULT

ABSTRACT

An interactive assistant, referred to herein as “an interactive assistant,” “a virtual assistant,” or simply “an assistant,” may be configured to securely store passwords, access codes, private keys, digital certificates, and other secret information. When the interactive assistant receives a request from the user to perform an action that requires the use of the secret information stored by the interactive assistant, the interactive assistant can provide such secret information to web sites, services, devices, systems, and the like to authenticate the interactive assistant to gain access to resources as part of performing the requested action. For example, when the interactive assistant encounters a website with username and password fields, the interactive assistant may retrieve the username and password associated with the website and may fill in the retrieved username and password into the username and password fields.

DESCRIPTION

An interactive assistant, such as shown in the example of Figure 1 below, may be included in a computing system that is configured to interact with one or more users. The computing system may be, include, or otherwise be included in a mobile device (e.g., smart phone, tablet computer, laptop computer, computerized watch, computerized eyewear, computerized gloves), a personal computer, a smart television, a personal digital assistant, a portable gaming system, a media player, a mobile television platform, an automobile navigation and/or entertainment system, a vehicle (e.g., automobile, aircraft) and/or cockpit display, or any other type of wearable, non-wearable, mobile, or non-mobile computing device, and the

computing system may or may not include a display device. In some cases, the interactive assistant may be a voice-assistant that receives audible user commands, processes the commands based on speech recognition operations, and performs corresponding actions, such as providing audible responses to user queries and/or performing certain actions. The interactive assistant may provide or utilize a user interface with which a user can communicate to cause the assistant to output useful information, respond to a user's queries, or otherwise perform certain operations to help the user complete a variety of real-world or virtual tasks.

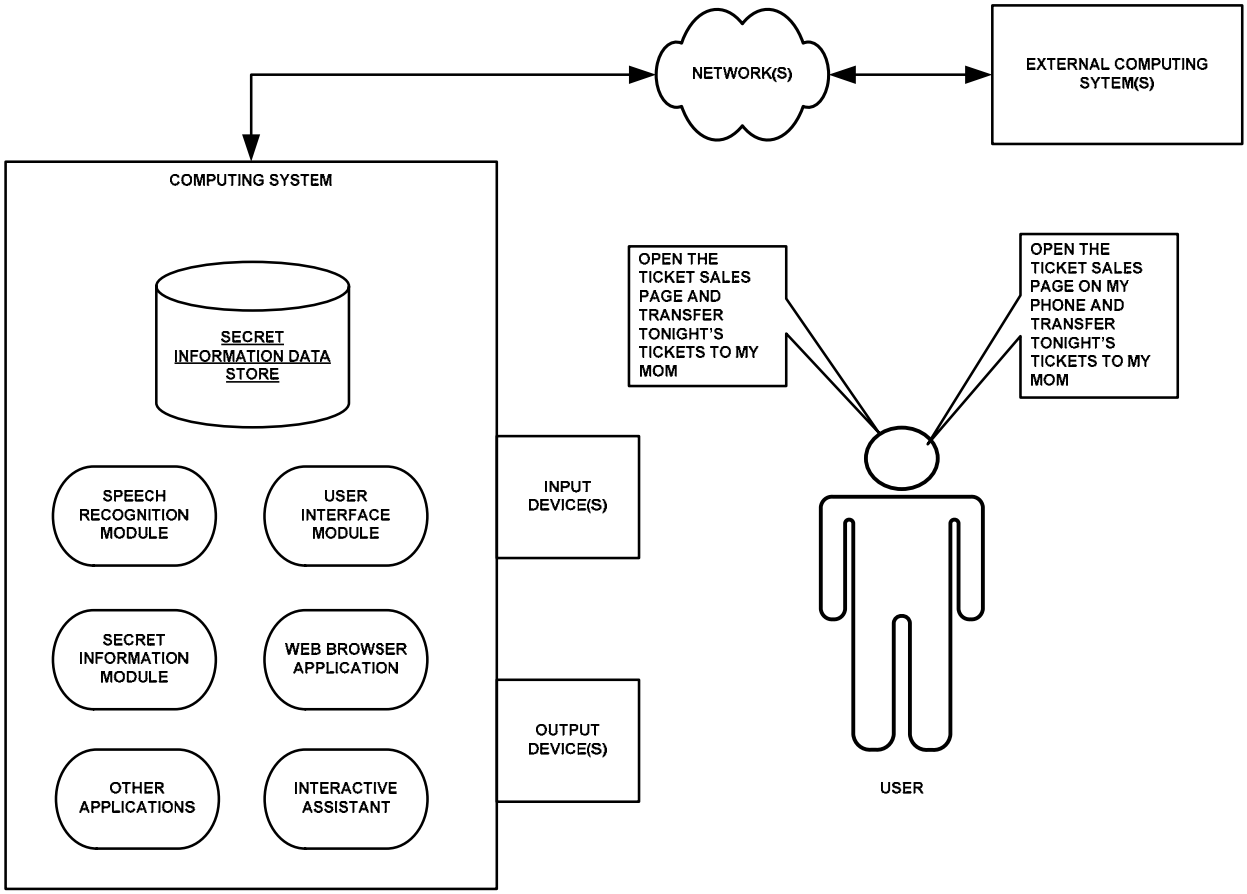

Figure 1

Figure 1 above illustrates an example of an interactive assistant that is configured to store secret information and to use the stored secret information to perform actions requested by a user. The computing system that includes the interactive assistant may have or otherwise be communicatively coupled to one or more input devices and one or more output devices. For instance, the input devices may include one or more microphones, a presence-sensitive input device (e.g., a touch-sensitive screen), a mouse, a keyboard, a voice responsive system, a camera, or any other type of device for detecting input from a human or machine. In some cases, the input device may one or more location sensors (GPS components, Wi-Fi components, cellular components), one or more temperature sensors, one or more movement sensors (e.g., accelerometers, gyroscopes), one or more pressure sensors (e.g., barometer), one or more ambient light sensors, and/or one or more other sensors (e.g., camera, infrared proximity sensor, hygrometer, and the like). Other sensors may include a heart rate sensor, magnetometer, glucose sensor, hygrometer sensor, olfactory sensor, compass sensor, step counter sensor, to name a few other non-limiting examples.

The computing system may also include or be communicatively coupled to one or more output devices, such as one or more speakers or display screens, including a presence-sensitive screen (e.g., touchscreen), or any other type of device for generating output to a human or machine. In some cases, the input devices and/or output devices may include one or more other type of wearable, non-wearable, mobile, or non-mobile computing devices that are also used by the user. One or more of the input and/or output devices may be external to and communicatively coupled (e.g., via a wired or wireless connection) with the computing system.

The computing system may also include a user interface module that is configured to manage inputs received by the interactive assistant as users interact with the computing system, and the user interface module may be configured to receive additional instructions from applications, services, platforms, or other modules of the interactive assistant that process user input. The user interface module may also be configured to process output that is provided to users, and may be coupled to the input device(s) and output device(s) of the interactive assistant. The computing system may also include a speech recognition module, which may interface with the user interface module and/or the interactive assistant. When a user provides audible input to the interactive assistant (e.g., via commands, questions, queries, and requests), the interactive assistant may use the speech recognition module to process such audible input.

The interactive assistant may store passwords, access codes, private keys, digital certificates, and other secret information for a user of the computing system. The secret information stored by the interactive assistant may be information used to authenticate the user of the interactive assistant and/or the computing system with third-party services, such as websites, applications, and the like.

Because the secret information may be associated with information that identifies the user, such as usernames, e-mail addresses, and the like, the interactive assistant may also store user identification information associated with the secret information. Thus, the interactive assistant may store a password, an associated username. Further, because secret information may be associated with a specific third-party service, the interactive assistant may also store, for a secret information, the third-party service associated with the password. Thus, the interactive assistant may store information that identifies the third-party service (e.g., a web site address, a

name, an ID, or other suitable third-party service identifier), user identification information for the third-party service (e.g., a user name, an e-mail address, a phone number, etc.), and an associated secret information (e.g., password, access code, biometric information, etc.) associated with the third-party service and the user name. For example, the interactive assistant may store a URL such as "http://www.example.com/login/," an associated username, and an associated password. In this way, when the web browser application visits the website, the interactive assistant may fill in the username and password fields with the associated username and password.

The computing system enables the user to control what information the interactive assistant can store in the secret information data store. For example, the interactive assistant may only be able to store information in the secret information data store if the user expressly permits the interactive assistant to do so. Thus, the interactive assistant may refrain from storing certain information into the secret information data store if the user does not give explicit permission for the interactive assistant to store the information.

The interactive assistant may receive secret information along with its associated user identification information and third-party service identifier for storage in the secret information data store in many ways. For example, when the user inputs a username and a password into the username and password fields of a website, the interactive assistant may store the inputted username and password along with the URL of the website. In another example, if another computing device associated with the user (i.e., a computing device other than the computing system) has a secret information data store, the user may enable the computing system to receive

secret information stored in the secret information data store, and to store the received secret information into the secret information data store in the computing system.

In some examples, the secret information data store may not be included in the computing system, but may be stored in a remote computing device (e.g., the cloud). Further, the secret information data store may be encrypted or otherwise secured to prevent unauthorized access to the secret information data store.

By storing such secret information and associated information, the interactive assistant can use the stored information to authenticate the user instead of requiring the user to input the secret information each time the computing system encounters a third-party service that requires user authentication via secret information. When the interactive assistant receives a request to perform an action, the interactive assistant may determine whether performing the requested action involves using the stored secret information to authenticate with a third-party service. If so, the interactive assistant determines whether it has stored secret information for authenticating the user with the third-party service. If the interactive assistant determines that it has stored secret information for authenticating the user with the third-party service, the interactive assistant can use the stored secret information to authenticate the user with the third-party service in order to perform the requested action.

The interactive assistant may receive a request from a user to perform one or more actions. To perform the one or more actions requested by the user, the interactive assistant may interact with a website or other third-party services. A website, app, or other third-party service may require users to authenticate or validate themselves by providing user identification information and secret information in order to grant the user access the third-party service. For

example, a banking web site may require a user to log in by providing a username and password. If the banking web site determines that the provided username is associated with an authorized user of the banking web site, and that the provided password is the valid password associated with the provided username, the banking web site may grant the user access to the banking web site. For example, the banking web site may grant the user the ability to view balances, perform wire transfers, order paper checks, and the like.

Because the interactive assistant can store secret information for the user, the interactive assistant may determine whether it stores an appropriate password to access a service and, if so, may provide the stored password as well as associated user identification information to the service to gain access to the service. For example, interactive assistant may “log in” to the service with a username and password associated with the service that are stored by the interactive assistant, such as by filling in the username and password fields of a website with the requisite username and password. By utilizing the stored username and password to automatically log into the service, the interactive assistant does not have to request the username and password from the user.

The interactive assistant may determine, based on the requested action, whether the requested action requires the interactive assistant to provide secret information and, if so, whether it has stored a suitable secret information for the requested action. For example, if, as part of performing the requested action, the interactive assistant encounters a webpage that requires a username and password to be entered, then the interactive assistant may determine whether it has stored secret information associated with the webpage.

If the interactive assistant determines that it has stored secret information associated with the third-party service, the interactive assistant may retrieve such secret information and may utilize the secret information, as well as information such as a username or e-mail associated with the secret information to perform the requested action. In the case of a webpage that requires a username and password to be entered, the interactive assistant may automatically retrieve and enter the appropriate username and password into the username and password fields of the webpage. That is, the interactive assistant may automatically retrieve and enter the appropriate username and password into the username and password fields of the webpage without user invention or user direction.

In one example, the user may issue a request for the interactive assistant to transfer concert tickets the user has for a concert tonight to the user's mother by vocally stating "open the ticket sales page and transfer tonight's tickets to my mom." A microphone of the computing system may receive the user's request. The speech recognition module of the computing system may perform speech recognition on the user's request and may provide the user's request to the interactive assistant.

The interactive assistant may attempt to identify the user that issued the request and to determine whether the user is authorized to issue a request that requires the interactive assistant to access the secret information data store. For example, the interactive assistant may perform voice authentication, speaker recognition, speaker verification, and the like to determine if the user is an authorized user of the interactive assistant. The interactive assistant may perform such authentication, recognition, verification, and the like by analyzing the audio of the user's request as received by the microphone of the interactive assistant and performing any suitable techniques

for authentication, recognition, verification, and the like to determine whether the user is authorized to issue a request that requires the interactive assistant to access the secret information data store. In other examples, the interactive assistant may be able to authenticate, recognize, and/or verify the user via any other suitable technique, such as by receiving secret information (a password, access code, other biometric information, etc.) that identifies the user as being authorized to issue a request that requires the interactive assistant to access the secret information data store.

If the interactive assistant is used by multiple users, the interactive assistant may be able to distinguish between multiple authorized users of the interactive assistant. The interactive assistant may be able to store sets of secret information for each of the authorized users in the secret information data store. The interactive assistant may identify, based on analyzing the audio of the user's request as received by the microphone of the interactive assistant or via any other suitable technique, the user that issued the request out of the multiple authorized users of the interactive assistant, and may be able to access only the secret information stored in the secret information data store for the identified user.

This may be useful when multiple authorized users of the interactive assistant store secret information associated with the same third-party service. By identifying the user that issued the request, the interactive assistant may use the appropriate secret information in the secret information data store that is associated with the user to perform the requested action.

The interactive assistant may perform the requested action by, in one example, using the web browser application to browse to a concert ticket sales website that allows the user to manage and transfer her concert tickets. When the web browser application loads the concert

ticket sales website, the interactive assistant may retrieve the username and password for the website from the secret information data store and may input the retrieved username and password into the username and password fields on the website. Once the interactive assistant successfully authenticates the user via the retrieved username and password, the interactive assistant may utilize the web browser application to access the ticket transfer functionality on the concert ticket sales website to transfer the user's concert tickets to the user's mom.

The interactive assistant may also be used to perform actions using computing devices that are external to the computing system using secret information stored by the computing system. For example, the user of the computing system may utilize a mobile phone that is external to the computing system. The user may issue a request for the interactive assistant to utilize the user's phone to transfer concert tickets the user has for a concert tonight to the user's mother by vocally stating "open the ticket sales page on my phone and transfer tonight's tickets to my mom." A microphone of the computing system may receive the user's request. The speech recognition module of the computing system may perform speech recognition on the user's request and may provide the user's request to the interactive assistant.

The interactive assistant may perform the requested action by, in one example, communicating with the external computing device (e.g., the user's phone) and directing the external computing device to use its web browser application to browse to a concert ticket sales website that allows the user to manage and transfer her concert tickets. When the web browser application loads the concert ticket sales website, the interactive assistant may retrieve the username and password for the website from the secret information data store, and may direct the external computing device to input the retrieved username and password into the username and

password fields on the website. Once the external computing device successfully authenticates the user via the retrieved username and password, the interactive assistant may direct the external computing device to utilize the web browser application to access the ticket transfer functionality on the concert ticket sales website to transfer the user's concert tickets to the user's mom.

It should be understood that the interactive assistant may be able to use the stored secret information in conjunction with applications other than web browser applications in order to authenticate the user of the computing system with a third-party service. For example, the user may request that the interactive assistant book her a ride with a ride sharing service by vocally stating "book me a ride to my dinner reservation." A microphone of the computing system may receive the user's request. The speech recognition module of the computing system may perform speech recognition on the user's request and may provide the user's request to the interactive assistant.

The interactive assistant may perform the requested action by interacting with a ride sharing service application to book a ride for the user. For example, the interactive assistant may retrieve the username and password of the user associated with the ride sharing service application from the secret information data store and may authenticate the user with the ride sharing service application using the retrieved username and password. Upon authenticating the user with the ride sharing service, the interactive assistant may direct the ride sharing service application to book a ride for the user to the location of her dinner reservation.