Technical Disclosure Commons

Defensive Publications Series

November 26, 2018

On-demand Multi-factor Authentication for Automated Assistant Interactions

Lilin Wang

David Roy Schairer

Mark Spates IV

On-demand Multi-factor Authentication for Automated Assistant Interactions

Abstract

Techniques set forth herein are related to on-demand dynamic requests for multi-factor authentication ("MFA") challenges, such as two factor authentication ("2FA") challenges. The MFA challenges can be selectively provided to a user in response to an interaction of the user with an automated assistant. In some instances, an MFA challenge is selectively provided by an automated assistant in response to a user interaction, with the automated assistant, that is an attempt to control a smart device of a third party, an attempt to transact with a third party, or other attempted interaction with a third party. In some of those instances, the automated assistant submits a corresponding request to a third party computer system of the third party, and the third party computer system dictates whether the MFA challenge is to be provided. For example, the third party computer system can either implement the corresponding request without requesting MFA, or can respond to the corresponding request with a request for the automated assistant to provide a MFA challenge (in which case the corresponding request will not be implemented unless an appropriate response to the MFA challenge is received).

Description

Multi-factor authentication ("MFA") is a technique to reliably confirm a user's identity by combining multiple factors. For example, two-factor authentication ("2FA") can combine: something the user has and something the user knows. An example of 2FA is withdrawing money from an automatic teller machine, where the user has a bank card (something the user has) and the user enters a PIN (something the user knows).

Currently, MFA requests in the automated assistant context either always happen or never happen. For example, MFA requests can always occur for certain third parties and/or for

certain types of automated assistant interactions. There is currently no mechanism for an automated assistant and/or a third party (to which an automated assistant request is directed) to dynamically decide on-demand whether an MFA request should be provided in response to a user interaction with an automated assistant.

Accordingly, techniques described herein enable on-demand dynamic determination of when to request MFA in response to a user interaction with an automated assistant. Some techniques can be utilized to dynamically request MFA in association with user requests to control smart devices, such as Internet of Things ("IoT") devices. As mentioned above, various techniques can enable a third party computer system associated with a smart device, such as a smart lock, to determine whether or not to request MFA challenges be provided by the automated assistant. In some instances, the third party computer system can decide whether or not to request MFA based on one or more contextual signals, such as signals that may be available to the third party computer system, but unavailable to the automated assistant. For example, a user, while standing next to his/her smart lock, can request that the smart lock be unlocked via providing a spoken request to the automated assistant (*e.g.*, a spoken utterance of "unlock the front door"). The user can be carrying a third party provided token that can be detected by the smart lock (but not the automated assistant), and the smart lock can transmit, to a third party computer system associated with the smart lock, an indication that the token is detected by the smart lock. In such an example, the automated assistant can transmit a command to the third party computer system requesting the smart lock be unlocked, and the third party system can unlock the smart lock without requesting MFA. The third party system can unlock the smart lock without requesting MFA based at least in part on the third party system receiving the indication that the token is detected. Alternatively, if the token and/or other signals are not

detected by the third party system, it can instead send a request that the automated assistant provide a MFA challenge. The automated assistant can provide the MFA challenge and receive user input in response (*e.g.*, spoken input, typed input, biometric input). The automated assistant itself can determine whether the user input satisfies the MFA challenge, or can provide the user input (or a conversion thereof) to the third party, which can determine whether the user input satisfies the MFA challenge. When the challenge is successful (as indicated by the automated assistant or as determined by the third party), the third party can then unlock the smart lock.

In some instances, a smart device can itself make on-demand MFA requests directly to the automated assistant. For example, a smart device itself can decide if it is going to send a request for MFA to an automated assistant, to thereby cause the automated assistant to perform MFA via an automated assistant interface. For instance, in response to a user request to unlock a smart lock, the smart device itself can decide if it will require the user to input a numerical code (*e.g.*, verbally and/or through touch input via an assistant interface) to unlock the lock based on the current situation instead of always requiring the user to input the numerical code. In some instances, the smart lock can decide to not require MFA when the smart lock detects certain conditions, such as a recognized phone of the homeowner being within a certain distance of the smart lock. Alternatively, when the smart lock decides MFA is required, it can send a request to the automated assistant that specifies an MFA challenge should be provided, and specifies that the MFA challenge should be a request for user input of a numerical code to unlock the door. The smart lock can unlock the door when it receives a response from the automated assistant that includes the numerical code (that the smart lock determines is correct), or that indicates the user has correctly provided the numerical code (as determined by the automated assistant).

In some instances, techniques described herein can additionally or alternatively facilitate

automated assistant interactions associated with third party provided services. For example, a user can request an automated assistant order a pizza from "Hypothetical Pizza Restaurant". The automated assistant can provide a corresponding agent request to a third party agent (*e.g.*, software operating on a third party computer system) that is associated with "Hypothetical Pizza Restaurant". The third party agent can on demand decide whether or not to request MFA in response to the corresponding agent request. If the third party agent associated with "Hypothetical Pizza Restaurant" determines MFA is required, the third party agent can send a request to the automated assistant for the user to provide (verbally and/or textually), for example, the last four digits of the credit card associated with the user's account and/or other multi-factor authentication input. Once the third party agent receives the last four digits of the credit card, it can process the payment and complete the pizza order.

Various instances of MFA described herein occur in response to a user engaging with interactive software applications that are referred to herein as "automated assistants", and that can also be referred to as "chat bots", "interactive personal assistants," "intelligent personal assistants", "personal voice assistants", etc. Users can provide commands, queries, and/or requests to automated assistants using natural spoken language input which may in some cases be converted into text and then processed, and/or by providing textual natural language input. Further, the automated assistants respond to a request from a user by providing an appropriate response and/or performing a particular task (*e.g.*, controlling an appropriate IoT device, initiating a transaction). In responding to requests, automated assistants can interface with various agents and/or smart devices, such as third party agents and/or smart devices.

Smart devices, as referred to herein, include various IoT devices. An IoT device can include one or more of: electronics, software, sensors, actuators, etc. These devices can connect

over a network to exchange information, and each device can be uniquely identifiable and operate within an existing network infrastructure. For example, an automated assistant can remotely control a variety of IoT devices including smart: thermostats, light bulbs, keyless door locks, doorbells, security cameras, electrical outlets, light switches, smoke detectors, flood sensors, vacuums, washers, dryers, window shades, dishwashers, security systems, fans, TV, etc.

In some instances, automated assistants can directly control a device. In other instances, third party agents (also referred to as "third party computer systems") can facilitate interactions between an automated assistant and a user, including controlling a device and/or providing a service to the user. Third party agents can be hosted on server(s) that are separate from those controlling the automated assistant and can control a variety of tasks including: turning on a smart light, unlocking a smart door lock, ordering a pizza, ordering a ridesharing vehicle, etc.

In view of these and/or other considerations, techniques described herein allow dynamic control of MFA challenges when communicating with an automated assistant. In some instances, MFA challenge requests transmitted to an automated assistant can include a request for a variety of information including: voice fingerprinting, facial identification, fingerprint recognition, eye iris recognition, typing pattern biometrics recognition, possession of a password (e.g. a four digit PIN), possession of a physical token within proximity of the automated assistant, possession of a software token, etc. In some instances, the device itself and/or the third party agent determines what kind of MFA challenge should be provided.

In some instances, a device itself can dynamically decide to make or not make a MFA request to an automated assistant in response to receiving a command from an automated assistant. For example, a smart thermostat can use MFA to limit access to the thermostat controls. Through the user interface on the smart thermostat, a user can set up password to grant

access to thermostat settings. In some instances, the user can give the automated assistant a verbal command to change the temperature on the thermostat. The thermostat can decide the owner of the device is giving the verbal command to change the temperature through voice fingerprinting-based authentication provided by the automated assistant and decide to not request MFA from the automated assistant. Alternatively, the thermostat can decide to that MFA is required, and send the automated assistant a request that the user needs to verbally speak the password to the automated assistant. When the thermostat receives confirmation from the automated assistant that the user has spoken the correct password, the thermostat can complete the user request to change the temperature.

In some instances, a third party agent associated with a device can dynamically decide to make or not make a MFA request to an automated assistant. For example, a third party agent can control a group of four smart lights within a kitchen. The smart lights can have customizable settings where all four lights automatically turn on at 6:00 am, all four dim to 75% at 7:30 pm, three of the lights turn off at 10:00, and the last remaining light turns off at midnight. If a user is having a party and wants to keep all four lights at 100% after 7:30 pm, the user can provide a verbal command to the automated assistant to change the light settings for all four lights in the kitchen.

The third party agent can decide if MFA is necessary for this command utilizing one or more automated assistant provided signals and/or signals that are directly determined by the third party agent. If the third party agent decides MFA is unnecessary, the third party agent can immediately change the lighting settings consistent with the verbal command. Alternatively, the third party agent can determine MFA is necessary to change the lighting settings, and the third party agent can send a request asking the automated assistant to prompt the user for a passphrase

and/or other information. The third party agent can change the lighting settings once it receives confirmation, from the automated assistant, that the user has provide the correct information.

In some instances, the user can accidentally speak the incorrect passphrase and the automated assistant can prompt the user for the passphrase again. If the user speaks the correct passphrase, the automated assistant can transmit conformation of the correct passphrase to the third party agent and the third party agent can complete the user request to change the light setting. In some instances, a maximum number of prompts for correct MFA challenge information can be set by either an automated assistant, a device, and/or a third party agent.

In some instances, a third party agent associated with a service can dynamically decide to make or not make a MFA request to an automated assistant. For example, a third party agent can order a ride for a user from Hypothetical Ridesharing Company. The user can provide the automated assistant a request to order a ride from Hypothetical Ridesharing Company to hypothetical destination. The automated assistant can transmit the rideshare request to the third party agent associated with Hypothetical Ridesharing Company along with other relevant information, such as the hypothetical destination and a current location of the user. If the third party agent determines MFA is required, it can send a request to the automated assistant for the user to verbally confirm the last four digits of the credit card number associated with the Hypothetical Ridesharing Company account. The third party agent can complete the ridesharing request and order a ridesharing vehicle once it receives, via the automated assistant, an indication of the four digits provided by the user, and confirms the provided four digits conform to the last four digits of the credit card associated with the account. In such an example, the automated assistant facilitates the MFA, but the third party agent performs the MFA based on information gathered via the automated assistant. In other situations, such as other examples described

herein, the automated assistant itself performs the MFA, and provides, to the third party agent, an indication of whether the MFA is successful.

FIG. 1 below illustrates a system diagram 100 that includes an example of one or more client devices 102. Client device 102 can include, for example, a display device, a desktop computer, a laptop computer, a tablet computer, a mobile phone, a computing device in a vehicle of the user, and/or a wearable device that includes a computing device (e.g. a watch with an integrated computing device, a virtual or augmented reality computing device, etc.). Client device 102 may execute a respective instance of an automated assistant client 108, and in some instances a user can engage with an automated assistant client 108 executing on client device 102. In some instances, an instance of an automated assistant client 108, by interacting with one or more cloud-based automated assistant components 116 via one or more local and/or wide area networks, indicated generally as 114, may form what appears to be from the user's perspective, a logical instance of an automated assistant 112. One such instance of an automated assistant 112 is depicted in FIG. 1 by a dashed line.

In some instances, automated assistant 112 can connect to one or more peripheral devices 104 (e.g. IoT devices, smart devices, etc.) via network 114 to facilitate transactions between a user and device 104. In other instances, automated assistant 112 can use the third party agent 106 to facilitate transactions between the user and device 104.

In some instances device 104 and/or third party agent 106 can dynamically decide when to make MFA requests with automated assistant 112. In other words, client device 104 and/or third party agent 106 can sometimes request MFA from automated assistant 112 but do not always have to request MFA from automated assistant 112. The decision of when to request MFA is up to device 104 and/or third party agent 106.

In some instances, automated assistant 112 may engage in a dialog session with one or more users via user interface and output devices of client device 102. In some instances, the user interface input is explicitly directed to automated assistant 112. For example, a user may speak a predetermined invocation phrase, such as "OK, Assistant", or "Hey, Assistant" to cause automated assistant 112 to begin actively listening. In some instances, a third party agent may decide to request MFA and request automated assistant 112 to prompt a user to speak a passphrase, type a pin (*e.g.*, via touchscreen), and/or perform other authentication before the third party agent will complete a user's command.

In some instances, each automated assistant client 108 may include a corresponding speech/capture/text-to-speech("TTS")/speech-to-text('STT") module 110. In other instances, one or more aspects of speech capture/TTS/STT module 110 may be implemented separately from the automated assistant client 108. In some instances, each speech capture/TTS/STT module 110 may be configured to perform one or more functions: capture a user's speech, e.g., via a microphone; convert that captured audio to text (and/or to other representations or embeddings); and/or convert text to speech. In other instances, speech input may be sent to cloud-based automated assistant components 116, which may include cloud-based TTS module 118 and cloud based STT module 120. Automated assistant client 108 can additionally or alternatively leverage non-speech based input modalities for interacting with the automated assistant 112. For example, a user can interact with a virtual keyboard on a touchscreen of the client device 102 to provide typed input to the automated assistant client 108, can interact with graphical interfaces (*e.g.*, interface element(s) for controlling a smart lock, smart lights, etc.) that are rendered on a touch screen, etc.

In some instances, cloud-based STT module 120 can leverage the virtually limitless

resources of the cloud to convert audio data captured by speech capture/TTS/STT module 110 into text (which may then be provided to natural language processor 122). Cloud-based TTS module 118 may be configured to leverage the virtually limitless resources of the cloud to convert textual data (e.g., natural language responses formulated by automated assistant 112) into computer-generated speech output.

In some instances, natural language processor 122 of automated assistant 112 processes natural language input generated by users via client device 102 and may generate annotated output for use by one or more components of automated assistant 112. In some instances, device 104 and/or third party agent 106 may receive output from natural language processor 122 via automated assistant 112 in determining if MFA is required, and can receive additional output if device 104 and/or third party agent 106 determines MFA is required. For example, a third party agent 106 can receive the output of user commands processed by the natural language processor 112 and use this information in determining what command has been requested by the user as well as determining if MFA is required in the particular situation. In some instances, if third party agent 106 determines MFA is required and the third party agent 106 determines it wants a spoken response from the user as the authentication challenge, natural language processor 122 can process the natural language input generated by the user and the output corresponding to the spoken response request from the third party agent 106 can be sent to the third party agent 106 by the automated assistant 112. In some instances, in response to user interaction with a graphical element (displayed on a touchscreen of client device 102) to control a smart device, the automated assistant 112 can provide a third party 106 with a corresponding command, and the third party agent 106 can determine whether MFA is required for performance of the corresponding command in the particular situation.

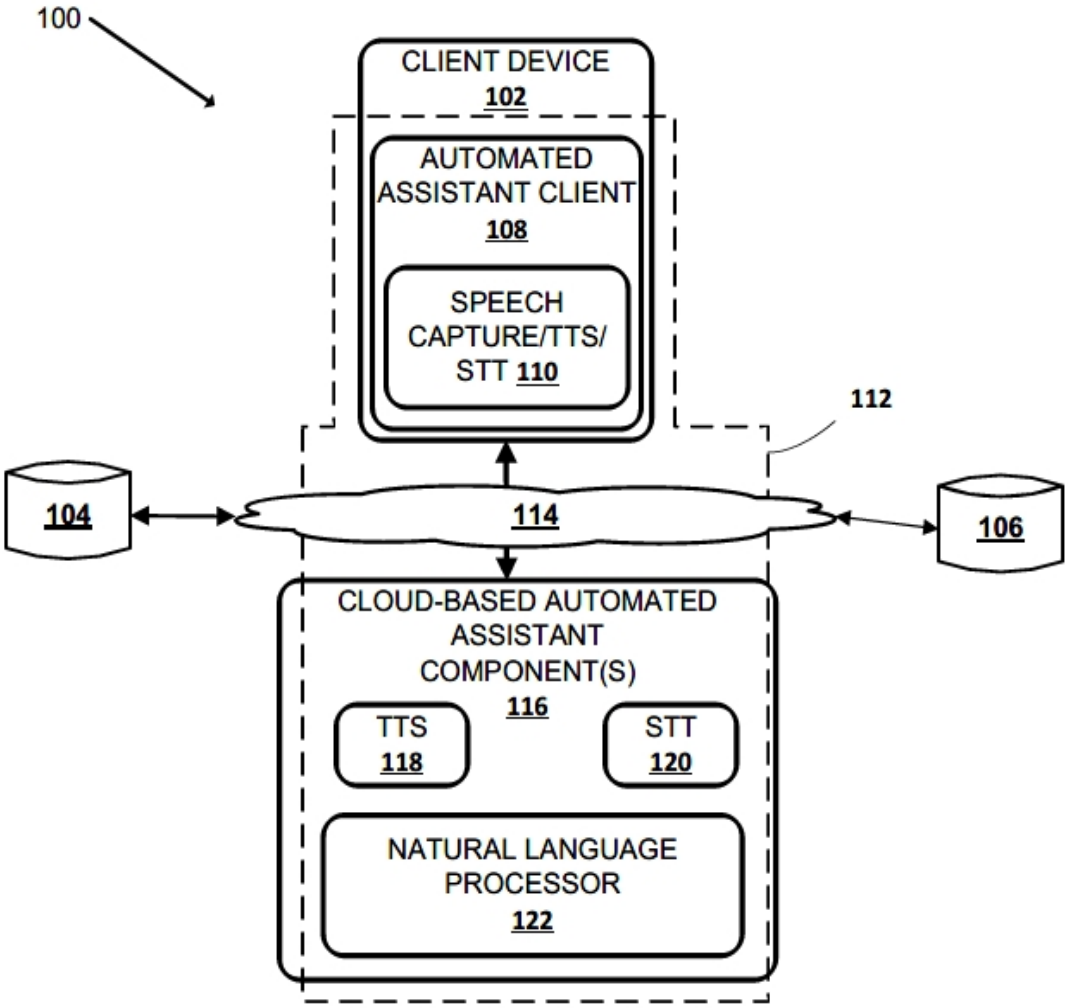
100
CLIENT DEVICE
102
AUTOMATED ASSISTANT CLIENT
108
SPEECH CAPTURE/TTS/ STT 110
112
104
114
106
CLOUD-BASED AUTOMATED ASSISTANT COMPONENT(S)
116
TTS
118
STT
120
NATURAL LANGUAGE PROCESSOR
122

Fig. 1