February 2021

IDENTIFYING VERIFIED BUSINESS CALLS USING TEMPORARY CONTACTS

Vinit Chandrakant Deshpande

IDENTIFYING VERIFIED BUSINESS CALLS USING TEMPORARY CONTACTS

ABSTRACT

A computing system (e.g., a cloud server) may cause a computing device to create a temporary contact profile that includes verified business contact information such that, when the verified business calls the computing device, the computing device can display the verified business contact information even if contact information for the business was not previously stored at the computing device. Responsive to receiving an incoming communication (e.g., a phone call, a text message, an instant message, etc.), the computing device may determine whether an address book or other contact repository of the computing device includes an entry for the originator (e.g., a business, a friend, a relative, etc.) of the incoming communication. Rather than requiring the user to have previously provided information for the originator of the incoming communication, techniques described herein may automatically create a temporary contact in the address book if the incoming communication originator is a verified business. Thus, even if the user has not previously created a contact profile for the verified business, the computing device may execute one or more applications to present a graphical user interface (GUI) that identifies the verified business using the information included in the contact profile, indicating to a user of the computing device the genuineness of the phone call.

DESCRIPTION

The present disclosure describes techniques for helping a user identify phone calls from a verified business by causing a computing device (e.g., smartphone, tablet, laptop, desktop, etc.) to create a temporary contact profile for a verified business that includes information received from a computing system. For example, the computing system may send the phone number,

name, logo, and the like of the verified business to the computing device. The computing device may then create and store a contact profile for the verified business that includes the information received from the computing system. Responsive to receiving a call from the verified business, the computing device may execute one or more applications to present a graphical user interface (GUI) that identifies the verified business using the information included in the contact profile, indicating to a user of the computing device the genuineness of the phone call.

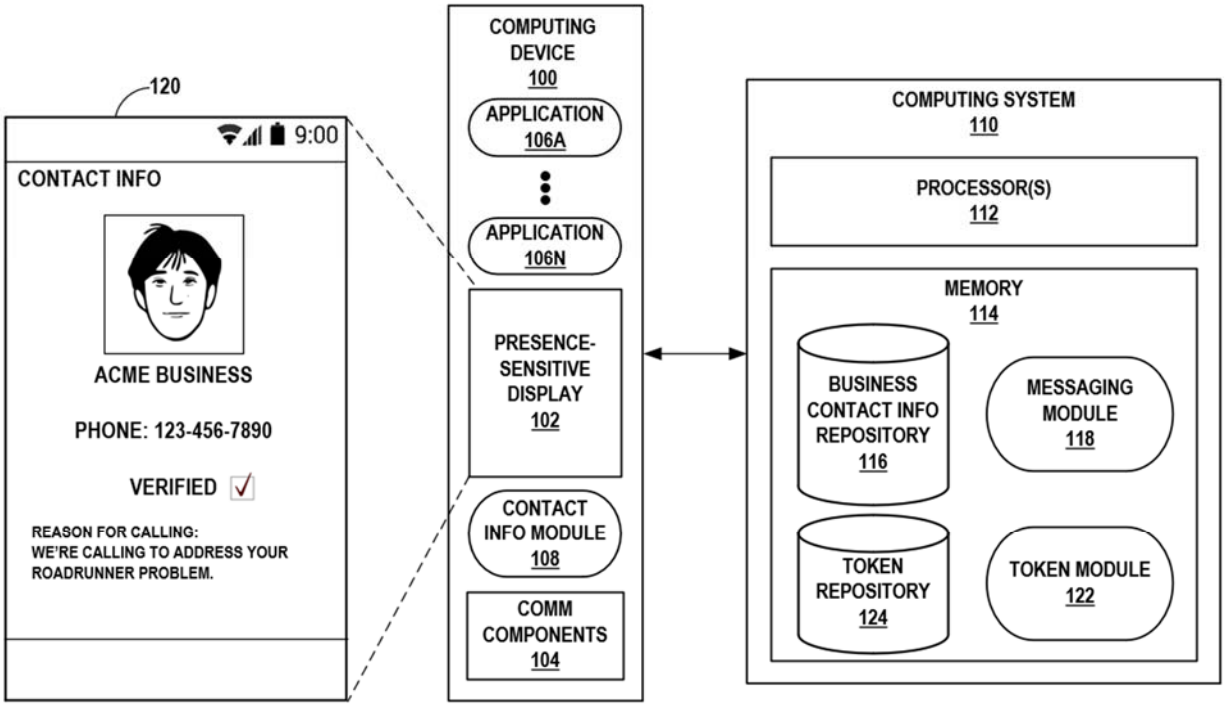

FIG. 1

FIG. 1 is a conceptual diagram illustrating a computing system 110 configured to enable a computing device 100 to verify the genuineness of incoming business phone calls. In the example of FIG. 1, computing device 100 is a mobile computing device. However, computing device 100 may be any mobile or non-mobile computing device, such as a cellular phone, a smartphone, a personal digital assistant (PDA), a desktop computer, a laptop computer, a tablet

computer, a portable gaming device, a portable media player, an e-book reader, a watch (including a so-called smartwatch), an add-on device (such as a casting device), smart glasses, a gaming controller, or another type of computing device that may pair with a Bluetooth® device.

Computing device 100 may include a display 102 and communication ("COMM") components 104. Display 102 may be a presence-sensitive display that functions as an input device and as an output device. For example, the presence-sensitive display may function as an input device using a presence-sensitive input component, such as a resistive touchscreen, a surface acoustic wave touchscreen, a capacitive touchscreen, a projective capacitive touchscreen, a pressure sensitive screen, an acoustic pulse recognition touchscreen, or another presence-sensitive display technology. The presence-sensitive display may function as an output (e.g., display) device using any of one or more display components, such as a liquid crystal display (LCD), dot matrix display, light emitting diode (LED) display, microLED display, organic light-emitting diode (OLED) display, e-ink, active matrix organic light-emitting diode (AMOLED) display, or similar monochrome or color display capable of outputting visible information (e.g., a GUI of a contact profile) to a user of computing device 100.

COMM components 104 may receive and transmit various types of information, such as information relating to the contact information of a caller. COMM components 104 may include wireless communication devices capable of transmitting and/or receiving communication signals via a network, such as a cellular radio, a 3G radio, a 4G radio, a 5G radio, a Bluetooth® radio (or any other personal area network (PAN) radio), a near-field communication (NFC) radio, a WiFi® radio (or any other wireless local area network (WLAN) radio), and/or the like. Additionally or alternatively, COMM components 104 may include wired communication

devices capable of transmitting and/or receiving communication signals via a direct link over a wired communication medium (e.g., a universal serial bus (USB) cable).

Computing system 110 may be any suitable remote computing system, such as one or more desktop computers, laptop computers, mainframes, servers, cloud computing systems, virtual machines, etc. capable of sending and receiving information via a network. In some examples, computing system 110 may represent a cloud computing system that provides one or more services (e.g., a cloud messaging service) via the network. That is, in some examples, computing system 110 may be a distributed computing system. One or more computing devices, such as computing device 100, may access the services provided by the cloud by communicating with computing system 110.

In the example of FIG. 1, computing system 110 includes one or more processors 112 and memory 114. Processors 112 may implement functionality and/or execute instructions associated with computing system 110. Examples of processors 112 include application processors, display controllers, auxiliary processors, one or more sensor hubs, and any other hardware configured to function as a processor, a processing unit, or a processing device. Modules (e.g., a messaging module 118, a token module 122, etc.) may be operable (or, in other words, executed) by processors 112 to perform various actions, operations, or functions of computing system 110. That is, modules may form executable bytecode, which when executed, cause processors 112 to perform specific operations in accordance with (e.g., causing computing system 110 to become a specific-purpose computer by which to perform) various aspects of the techniques described here.

Memory 114 may store application update repository 116, messaging module 118, token module 122, and token repository 124. Memory 114 may, in some examples, be described as a

computer-readable storage medium. For example, memory 114 may be configured for long-term, as well as short-term storage of information, such as instructions, data, or other information used by computing device 100. In some examples, memory 114 may include non-volatile storage elements. Examples of such non-volatile storage elements include magnetic hard discs, optical discs, solid state drives, flash memories, forms of electrically programmable memories (e.g., EPROMs), or electrically erasable and programmable memories (e.g., EEPROMs), as well as other forms of non-volatile memories known in the art.

In other examples, in place of, or in addition to the non-volatile storage elements, memory 114 may include one or more so-called "temporary" memory devices, meaning that a primary purpose of these devices may not be long-term data storage. For example, the devices may comprise volatile memory devices, meaning that the devices may not maintain stored contents when the devices are not receiving power. Examples of volatile memory devices include random access memories (RAM), dynamic random-access memories (DRAM), static random-access memories (SRAM), and other forms of volatile memories, or memory devices, known in the art. In some examples, the devices may store program instructions for execution by processors 112. For example, the devices may be used by modules 116-124 executing on computing device 100 to temporarily store information during program execution.

In accordance with techniques of this disclosure, computing system 110 may send (e.g., via one or more network packets) information including the business contact information of a verified business, which may cause computing device 100 to create a temporary contact profile to help a user determine the genuineness of incoming business phone calls. Computing system 110 may store the business contact information of a verified business in a business contact information repository 116 (hereinafter referred to as "BCI repository 116"). The business

contact information may include the name, phone number, logo, and/or the like of the business. Additionally, the business contact information may include the business's reason for calling a user of computing device 100.

Computing system 110 may execute messaging module 118 to generate one or more messages that include at least a portion of the business contact information (e.g., phone number, name, logo, etc.) of the verified business. Messaging module 118 may receive the business contact information from BCI repository 116. Computing system 110 may send the message(s) (e.g., as one or more network packets) to computing device 100 via a network. For example, computing system 110 may use a messaging service such as a cloud messaging service. The messaging service may be a cross-platform messaging service so that various computing devices (e.g., with different operating systems) may process the message(s) received from computing system 110.

Responsive to receiving (e.g., via COMM components 104) the message(s), computing device 100 may execute a contact info module 108 to create and store (e.g., in one or more storage devices) a contact profile of the verified business on computing device 100. The contact profile may include the name, phone number, logo, and/or the like of the verified business. For example, as shown in a GUI 120 of the contact profile, the contact profile for a verified business may include the verified business's logo (e.g., the headshot), name (e.g., "ACME BUSINESS"), phone number (e.g., "123-456-7890"), verification status (e.g., indicated by a text, an icon such as a checkmark, etc.), reason for calling (e.g., "to address a roadrunner problem"), and/or the like. In this way, computing system 110 may cause computing device 100 to create a contact profile that includes the business contact information of the verified business such that, when the verified business calls computing device 100, computing device 100 can display the business

contact information even if the business contact information was not previously stored at computing device 100.

One or more applications 106 of computing device 100 may monitor for a phone call from the verified business. For example, application 106A may be a dialer application configured to receive (e.g., via COMM components 104) phone calls. Responsive to receiving an incoming communication (e.g., a phone call, a text message, an instant message, etc.), contact info module 108 may determine whether an address book or other contact repository of computing device 100 includes an entry for the originator (e.g., a business, a friend, a relative, etc.) of the incoming communication. Responsive to contact info module 108 determining that the address book or other contact repository of computing device 100 includes an entry for the originator of the incoming communication, computing device 100 may use one or more applications 106 to display GUI 120 that identifies the originator using the information included in the contact profile associated with the entry for the originator. For example, application 106A may cause display 102 to present GUI 120. Thus, if the originator is a verified business, computing device 100 may execute application 106A to present GUI 120 that identifies the verified business using the information included in the contact profile, indicating to the user of computing device 100 the genuineness of the phone call.

Responsive to the satisfaction of a condition, computing device 100 may delete the contact profile of the verified business so that the contact profile is temporarily stored on computing device 100. For example, responsive to the termination of the phone call from the verified business, computing device 100 may delete the contact profile of the verified business. In another example, responsive to the lapse of a predetermined time period (e.g., a day, week, month, etc.), computing device 100 may delete the contact profile of the verified business.

In some examples, computing system 110 may use one or more tokens to authenticate the user of client device 100, thereby preventing malicious entities from impersonating the user. The tokens may include a public (e.g., available to the public) token identifying an intended recipient of a phone call. The tokens may further include a private (e.g., only available to a specific computing device) token authenticating the identity of the intended recipient.

For example, computing system 110 may use a token module 122 to create a public token and private token for computing device 100 and store the public token and private token in token repository 124. Computing system 110 may send the public token and private token to computing device 100 for computing device 100 to bear. Because the public token is available to the public and identifies an intended recipient of a phone call, the verified business may obtain (e.g., from token repository 124) the computing device's public token and send the computing device's public token to computing system 110 as part of a request to arrange a phone call between the verified business and the user of computing device 100.

Additionally, computing device 100 may send computing device's public token and private token to computing system 110 and request that computing system 110 send any phone call for computing device's public token to computing device 100. Token module 122 may use computing device's private token to authenticate computing device 100 as the original bearer of computing device's public token, and thus the intended recipient of the phone call. Responsive to token module 122 authenticating computing device 100, computing system 110 may send any phone call for computing device's public token to computing device 100.

One or more advantages of the techniques described in this disclosure may include re-instilling user confidence in telephony interactions by helping the user identify spam calls and phone scams. For example, if a computing device does not display a contact profile for a caller

during a phone call, the user may determine that the likelihood of the phone call being a spam call and/or a phone scam is high. Alternatively, if the computing device displays a GUI indicating that the originator of a phone call is a verified business, the user may determine that the likelihood of the phone call being a spam call and/or a phone scam is low and feel more comfortable sharing confidential information such as the user's credit card information, social security number, and/or the like. Further, these techniques may reduce impersonation attacks by using one or more tokens to authenticate the user of the client device. Such security measures may also re-instill user confidence in telephony interactions. Techniques described herein may also enable a computing device to automatically create a contact profile for the verified business, which may save the user's time and ensure the accuracy of the contact profile.

References

1. US Patent Application Publication No. US20200259954A1
2. KR Patent Application Publication No. KR20160093761A
3. KR Patent Application Publication No. KR20160044843A
4. Modak, "Google introduces 'Verified Calls' Feature on Google Phone App." TechnoSports, June 30, 2020.