August 02, 2019

TELEPHONE NUMBER ANTI-SPOOFING SYSTEM

Jian Yao

Dimitris Dimitropoulos

TELEPHONE NUMBER ANTI-SPOOFING SYSTEM

ABSTRACT

Communication service providers, such as mobile network providers, plain old telephone service (POTS) providers (e.g., landline providers), and/or Voice over Internet Protocol (VoIP) providers, provide telephone services. A communication service provider operates a computing system that connects calls from a caller to a recipient. The computing system authenticates a caller's telephone number to determine whether the telephone number is authentic or legitimate to prevent a caller from spoofing or faking his or her telephone number. The calling device places a call over a protocol that includes the telephone number of the sending device and an encrypted security key. The computing system utilizes the encrypted security key to verify or authenticate the identity of the caller. In other words, the computing system verifies the identity of the sender based on the encrypted security key to prevent robocalls that provide false telephone numbers and that are intended to spam, trick, deceive, or scam a call recipient. In some examples, if the computing system is unable to authenticate the identity of the caller, the computing system outputs a warning to the recipient of the call indicating that the caller's identity has been spoofed or is not authentic.

DESCRIPTION

Techniques are described that enable a computing system to authenticate the identity of a caller prior to transmitting a call to a recipient. In contrast to systems that enable a caller to specify any telephone number the caller wants, such that the caller may spoof a telephone number that is not the telephone number the caller is actually calling from, techniques of this

disclosure describe a new protocol that enables the computing system to reduce or eliminate the ability of a caller to spoof the caller's telephone number.

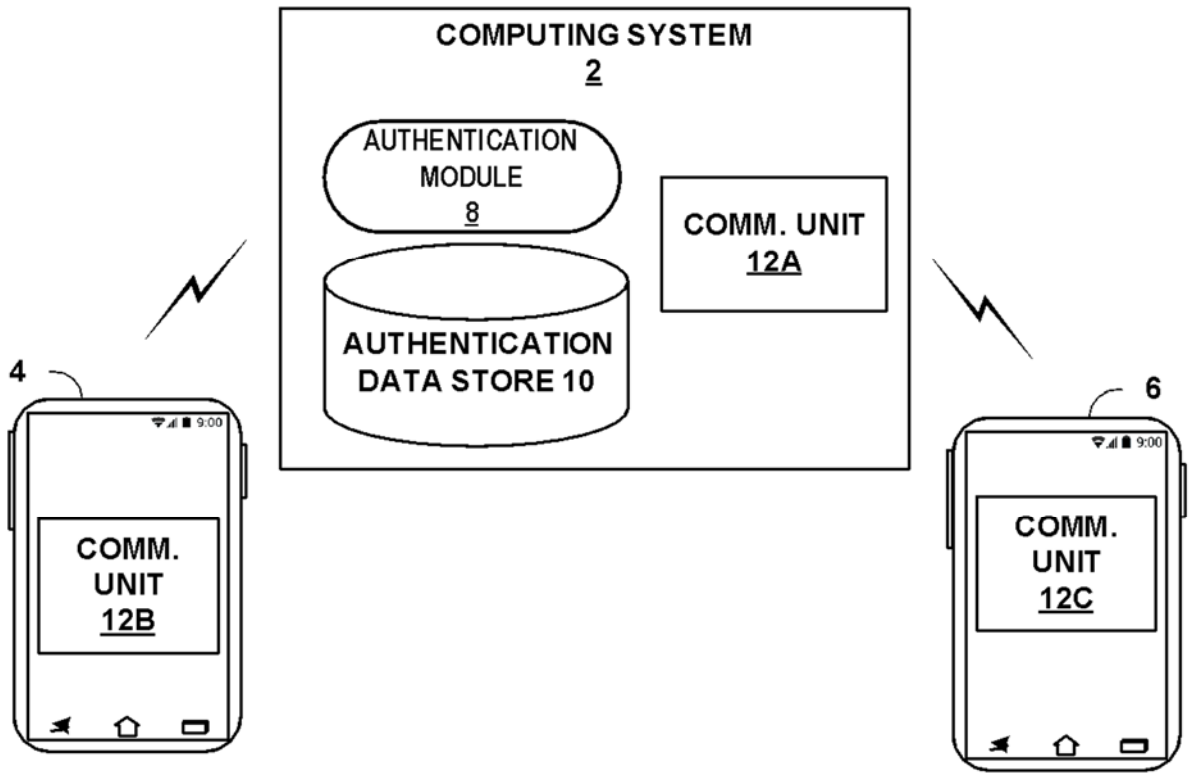

FIG. 1

In the example of FIG. 1, computing system 2 is configured to receive a telephone call from telephone 4 and communicatively couple telephone 4 to telephone 6. While telephones 4, 6 are illustrated as mobile phones (e.g., smart phones), in some examples, telephones 4, 6 may include any type of device capable of communicating with another device over a network, such as a desktop computer, a laptop computer, a tablet computer, a smart watch, or a smart speaker, among others. Examples of computing system 2 include, but are not limited to, servers, distributed computing systems (e.g., cloud-based computing systems), desktop computers, laptop computers, etc. Computing system 2, and optionally telephones 4, 6, include one or more processors. Examples of processors include, but are not limited to, digital signal processors

(DSPs), general purpose microprocessors, application specific integrated circuits (ASICs), field programmable logic arrays (FPGAs), or other equivalent integrated or discrete logic circuitry. In the example of FIG. 1, one or more processors execute the functionality of authentication module 8 of computing system 2.

Computing system 2 and telephones 4, 6 include communication units 12A-12C, respectively. Examples of communication units 12A-12C (collectively, communication units 12) include a cellular radio, a wireless network radio (e.g., WIFI™, BLUETOOTH ®), a network interface card (e.g. such as an Ethernet card), a cable modem, or any other type of device that can send and/or receive information. For example, communication units 12 may communicate over plain old telephone service (POTS), voice over internet protocol (VoIP), or wireless networks such as GSM, CDMA, LTE, etc.

Telephone 4 may send a request to computing system 2 to call telephone 6. Telephone 4 may send the request via a network protocol that specifies the telephone number of the recipient (e.g., the telephone number associated with telephone 6) and authentication information for telephone 4 and/or a user of telephone 4. For example, the authentication information may include the caller's telephone number (e.g., the telephone number associated with telephone 4) and a secret key. In one example, rather than including the secret key, the authentication information may include a hash of the secret key. In some examples, telephone 4 encrypts the authentication information prior to transmitting the authentication information to computing system 2.

Computing system 2 receives the request from telephone 4 to place a call to telephone 6. Computing system 2 receives the authentication information for telephone 4 and determines whether the caller's telephone number is authentic prior to connecting the call to telephone 6.

Computing system 2 determines whether the caller's telephone number is authentic based on the authentication information received from telephone 4 and authentication information stored within authentication data store 10. Authentication data store 10 may include data indicating a plurality of telephone numbers and, for each telephone number, a secret key or passcode. In other words, authentication data store 10 includes data associating each telephone number with a respective secret key. In one example, the secret key may be hardcoded to telephone 4 at the time of manufacture. In another example, the secret key may be generated by computing system 2 and stored by telephone 4 the first time the telephone number used by telephone 4 is activated. In yet another example, the secret key may be chosen by a user of telephone 4 or an application executing at telephone 4. In some examples, computing system 2 may store a hash of the secret key rather than storing the secret key itself.

Authentication module 8 of computing system 2 determines whether the telephone number provided by telephone 4 is authentic based on authentication data store 10. For example, authentication module 8 may query authentication information data store 10 to determine whether the combination of the telephone number and secret key provided by telephone 4 match the combination of the telephone number and secret key stored within authentication data store 10. In one example, authentication module 8 determines that the telephone number received from telephone 4 is authentic (e.g., the caller is who the caller purports to be) in response to determining that the secret key stored within authentication data store 10 for the received telephone number matches the secret key received from the caller.

Computing system 2 may communicatively couple telephone 4 and telephone 6 in response to authenticating the telephone number of the caller. That is, when computing system 2 determines that the caller is the legitimate owner of the telephone number, computing system 2

forwards the call to the telephone 6. In some such examples, computing system 2 transmits a notification to telephone 6 indicating that the telephone number has been verified and is authentic.

In another example, authentication module 8 determines that the telephone number received from telephone 4 is not authentic (e.g., the caller is using a spoofed telephone number) in response to determining that the secret key stored within authentication data store 10 for the received telephone number does not match the secret key received from telephone 4. That is, computing system 2 may determine that the caller is not the legitimate owner of the telephone number. In one example, computing system 2 refrains from forwarding the call to telephone 6 if computing system 2 determines the caller is not the legitimate owner of the telephone number provided by telephone 4. In another example, computing system 2 may forward the call to telephone 6 and may output a notification to telephone 6 indicating the telephone number was determined to be inauthentic. For example, the notification may indicate the call is a suspected spam call.

In one example, telephone 6 may automatically send the call to voicemail in response to receiving a notification indicating the telephone number is not authentic. In another example, telephone 6 may output a graphical user interface indicating the call is not authentic. In such examples, telephone 6 may provide the user of telephone 6 an option to screen the call, ignore the call, or answer the call.

By authenticating the telephone number of a caller, computing system 2 may increase user confidence that the caller is who the caller purports to be. Notifying call recipients that a caller is not who he or she purports to be may improve the user experience by enabling the recipient to screen or ignore spam calls. Furthermore, informing call recipients that the caller's

telephone number is not authentic may reduce fraud, for example, by reducing the probability the recipient unintentionally provides personal or financial information to unauthorized third parties.

REFERENCES

1. U.S. Patent Publication No. 2017/2,644,43 entitled "Systems and methods for authenticating caller identity and call request header information for outbound telephony communications" by Tu, et al.