TECHNIQUES FOR CALL AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/517,074, entitled "TECHNIQUES FOR CALL AUTHENTICATION" filed on July 19, 2019 (issued as U.S. Patent No. 10,506,426 on December 10, 2019). The contents of the aforementioned patent application are incorporated herein by reference in their entirety.

BACKGROUND

[0002] Unsolicited phone calls present an annoyance and a security risk for call recipients. Recipients may be subject to nuisance calls such as telemarketing calls, prank calls, and/or silent calls. Unsolicited calls may also be used to initiate telephone frauds, wherein imposters pose as legitimate entities in an attempt to steal information or funds.

[0003] Telephone call authentication involves attempting to identify a calling party. However, current methods lack the ability to reliably authenticate the devices called from and the parties calling from them. Furthermore, such methods are at best sparsely implemented and subject to practices such as spoofing, in which a caller may use a false identity and/or number in order to trick a call recipient into answering. As a result, users often have a mistrust of communication systems at best. At worst, they may be subject to nuisances and/or security risks.

SUMMARY

[0003a] According to a first aspect of the present invention, there is provided a computing device, comprising:

a memory configured to store instructions; and

processing circuitry coupled with the memory, the processing circuitry configured to execute the instructions, and when executed, the instructions to cause processing circuitry to:

determine to establish a communication connection with a second computing device;

generate an encrypted payload with a key and a cryptographic algorithm, the encrypted payload comprising an identifier to uniquely identify the computing device;

send the encrypted payload and a call number to service provider system to initiate establishment the communication connection with the second computing device; and

establish the communication connection with the second computing device based on a successful authentication performed by the service provider system utilizing the encrypted payload including the identifier.

[0003b] According to a second aspect of the present invention, there is provided a computer-implemented method, comprising:

a memory configured to store instructions; and

determining, by a processor of a computing device, to establish a communication connection with a second computing device;

determining encrypted payload, the encrypted payload comprising an identifier to uniquely identify the computing device encrypted with a key and a cryptographic algorithm;

sending the encrypted payload and a call number to service provider system to initiate establishment the communication connection with the second computing device, wherein the call number is associated with the second computing device; and

communicating, via the communication connection, with the second computing device based on a successful authentication performed by the service provider system utilizing the encrypted payload including the identifier.

[0003c] According to a third aspect of the present invention, there is provided a computer-readable medium storing instructions, the instructions configured to, when executed, cause one or more processors of a first computing device to:

determine to establish a communication connection with a second computing device;

determine encrypted payload, the encrypted payload comprising an identifier to uniquely identify the computing device encrypted with a key and a cryptographic algorithm;

send the encrypted payload and a call number to service provider system to initiate establishment the communication connection with the second computing device, wherein the call number is associated with the second computing device; and

communicate, via the communication connection, with the second computing device based on a successful authentication performed by the service provider system utilizing the encrypted payload including the identifier.

[0004] There is disclosed a method for performing peer to peer authentication of calls includes the steps of receiving an incoming call data stream from a first mobile phone device, the incoming call data stream comprising an incoming call number of a second mobile phone device and an encrypted payload comprising payload data encrypted using a private key associated with the first mobile phone device. In some embodiments, the private key comprises a dynamic key of the first mobile phone device and the encrypted payload comprises a cryptogram. The method may include authenticating the incoming call data stream in response to a match between the encrypted payload and stored information related to the first mobile phone device. In various aspects, the authentication includes forwarding the cryptogram to an authentication server, wherein the authentication

server maintains and modifies a copy of the dynamic key concurrently with the first mobile phone device as the stored information related to the first mobile phone device. In some embodiments, the authentication further includes receiving a validation of the first mobile phone device from the authentication server in response to a counter match between a counter extracted from the cryptogram using the copy of the dynamic key and an expected counter associated with the first mobile phone device. The

method may further include selectively establishing a call connection between the first mobile phone device and the second mobile phone device in response to the step of authenticating.

[0005] There is disclosed a system for authenticating calls between devices comprises an interface configured to receive an incoming call data stream from a first mobile phone device. In some embodiments, the incoming call data stream comprises an incoming call number associated with a second mobile phone device and an encrypted payload comprising payload data encrypted using a private key associated with the first mobile phone device. In some embodiments, the system includes a processor coupled to the interface and a non-volatile memory having program code stored thereon, the program code operable when executed upon by the processor to authenticate the incoming call data stream in response to a match between information of the encrypted payload and stored information related to the first mobile phone device. The system further includes a communication interface coupled to the processor and configured to selectively establish a call connection between the first mobile phone device and the second mobile phone device in response to the step of authenticating.

[0006] There is disclosed a method for authenticating calls between mobile devices includes the steps of receiving an incoming call data stream from a first mobile phone device. In some embodiments, the incoming call data stream comprises an incoming call number associated with a second mobile phone device, and an encrypted payload comprises payload data encrypted using a private key associated with the first mobile phone device and a voice message an attribute. The method includes retrieving a public key of the incoming call number from a data storage device and decrypting the encrypted payload using the public key of the incoming call number to produce a decrypted payload comprising an identifier. The method includes comparing the identifier of the decrypted payload to an expected identifier associated with the incoming call number to determine a first factor authentication match and comparing the attribute of the voice message to an expected voice message attribute to identify a second factor authentication match. The method further includes selectively establishing a connection between the first mobile phone device and the second mobile phone device in response to the first factor authentication match and the second factor authentication match.

[0007] With such an arrangement, a system and method are provided for reliably authenticating incoming calls.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] **FIG. 1** is a first block diagram of a data transmission system configured to authenticate user calls according to an example embodiment;

CLAIMS

1. A computing device, comprising:

a memory configured to store instructions; and

processing circuitry coupled with the memory, the processing circuitry configured to execute the instructions, and when executed, the instructions to cause processing circuitry to:

determine to establish a communication connection with a second computing device;

generate an encrypted payload with a key and a cryptographic algorithm, the encrypted payload comprising an identifier to uniquely identify the computing device;

send the encrypted payload and a call number to service provider system to initiate establishment the communication connection with the second computing device; and

establish the communication connection with the second computing device based on a successful authentication performed by the service provider system utilizing the encrypted payload including the identifier.

2. The computing device of claim 1, wherein the identifier comprises on one or more of password information, answers to pre-stored queries, biometric information, an image, or combination thereof.

3. The computing device of claim 1, wherein the identifier comprises audio data, and the audio data is unique to an expected user of the computing device.

4. The computing device of claim 1, wherein the call number is associated with the second computing device to establish the call communication connection with the second computing device.

5. The computing device of claim 1, wherein the key is a private key of a key pair, and the service provider system to decrypt the encrypted payload with a public key of the key pair to authenticate the identifier.

6. The computing device of claim 1, wherein the memory further comprises the key and the identifier, and the processing circuitry to retrieve the key and the identifier from the memory to generate the encrypted payload.

7. The computing device of claim 1, wherein the service provider system comprises a Voice over Internet Protocol (VoIP) network, a Public Switched Telephone Network (PSTN), or a combination thereof.

8. A computer-implemented method, comprising:
a memory configured to store instructions; and

determining, by a processor of a computing device, to establish a communication connection with a second computing device;

determining encrypted payload, the encrypted payload comprising an identifier to uniquely identify the computing device encrypted with a key and a cryptographic algorithm;

sending the encrypted payload and a call number to service provider system to initiate establishment the communication connection with the second computing device, wherein the call number is associated with the second computing device; and

communicating, via the communication connection, with the second computing device based on a successful authentication performed by the service provider system utilizing the encrypted payload including the identifier.

9. The computer-implemented method of claim 8, wherein the identifier comprises on one or more of password information, answers to pre-stored queries, biometric information, an image, or combination thereof.

10. The computer-implemented method of claim 8, wherein the identifier comprises audio data, and the audio data is unique to an expected user of the computing device.

11. The computer-implemented method of claim 8, wherein the identifier comprises data received from a contactless card.

12. The computer-implemented method of claim 8, comprising receiving, from a contactless card, the encrypted payload comprising the identifier, wherein the encrypted payload is generated by the contactless card utilizing the key and the cryptographic algorithm.

13. The computer-implemented method of claim 12, wherein the encrypted payload is received in a message authentication code (MAC) cryptogram.

14. The computing-implemented method of claim 12, wherein the encrypted payload is received via near-field communication (NFC) interface as part of an NFC exchange with the contactless card.

15. The computer-implemented method of claim 14, comprising sending an NFC read to the contactless card to request the encrypted payload and cause generation of a message authentication (MAC) cryptogram to communicate the encrypted payload.

16. The computer-implemented method of claim 8, wherein the key is a private key of a key pair, and the service provider system to decrypt the encrypted payload with a public key of the key pair to authenticate the identifier.

17. The computer-implemented method of claim 8, comprising:

storing, in a memory of the computing device, the key and the identifier;

retrieving, by a processor of the computing device, the key and the identifier; and

generating the encrypted payload by applying the cryptographic algorithm and the key to the identifier.

18. The computer-implemented method of claim 8, wherein the service provider system comprises a voice over Internet Protocol (VoIP) network, a public switched telephone network (PSTN), or a combination thereof.

19. A computer-readable medium storing instructions, the instructions configured to, when executed, cause one or more processors of a first computing device to:

determine to establish a communication connection with a second computing device;

determine encrypted payload, the encrypted payload comprising an identifier to uniquely identify the computing device encrypted with a key and a cryptographic algorithm;

send the encrypted payload and a call number to service provider system to initiate establishment the communication connection with the second computing device, wherein the call number is associated with the second computing device; and

communicate, via the communication connection, with the second computing device based on a successful authentication performed by the service provider system utilizing the encrypted payload including the identifier.

20. The computer-readable medium of claim 19, further comprising instructions to cause the one or more processors to:

retrieve the key and the identifier from memory; and

generate the encrypted payload by applying the cryptographic algorithm and the key to the identifier.