(54) Title: VOICE-BASED AUTHENTICATION OVER A NOISY CHANNEL

(57) Abstract: A remote communication terminal for verified communication, the terminal comprising: a sound input, a password encoder connected to said sound input for encoding a password identified from said sound input for resilience in a noisy channel, and a password output connected to said password encoder for sending said resiliently encoded password over a noisy channel to an authenticator. Also a verification apparatus for verifying the encoded password.
Voice-Based Authentication Over A Noisy Channel

Field of the Invention

The present invention relates to voice-based authentication over a noisy channel.

Background of the Invention

Remote communication is a major feature of modern life and it is now common to provide transaction facilities such as telephone banking, which require authentication of the user. Authentication is typically carried out by asking the user for a password. The password may be a word or a number or a combination of letters and numbers, which can either be given orally to service provider personnel or can be entered through the telephone keyboard and transferred using DTMF tones. If the communication is made via the Internet or via a messaging system then password entry is equally straightforward and may for example be carried out using an on-screen dialog.

If telephony devices are used then it is generally easiest to use passwords comprising numerical characters only, although such passwords are not necessarily easy to remember. There is thus a motivation to provide passwords that can be spoken.

A development in authentication enables automatic authentication of spoken or voice passwords. Such automatic authentication can be carried out in two ways. A first way is to use conventional voice recognition and authentication technology to match a spoken password against a stored password to determine that the correct password has been spoken. The voice authentication technology retains a copy of the correct password and calculates a statistical distance between a received word and the stored copy. Provided that the statistical distance is below a predetermined threshold the password is considered recognized.

In an alternative authentication system it is not a password but rather the speaker himself that is identified in the authentication process. Every speaker has a distinct voiceprint, which is machine identifiable, and the speaker is requested to speak
a word or phrase, allowing distinctive features of the speech, namely the voiceprint to be identified.

Both of the above systems of identification require that a reasonably clear, that is to say noise free and undistorted, version of the password or spoken phrase is received by the voice recognition and authentication apparatus. In general, however, voice channels are configured to provide a level of protection against noise and distortion which is sufficient for comprehension by the human ear. The voice channel does not necessary provide a quality of received signal that is sufficient for automatic voice recognition and authentication. In particular, cellular channels are configured to maximize the number of users by minimizing bandwidth, thus effectively working at maximal acceptable levels of noise and distortion within the channel. Thus signal quality, especially when the channel maximum capacity is reached and inter-user interference takes effect, can easily be insufficient to allow reliable automatic password authentication.

Summary of the Invention

It is an object of the present embodiments to provide reliable voice based authentication, which retains its reliability even when the voice signal to be authenticated is transferred over channels having relatively high noise and or distortion levels.

According to a first aspect of the present invention there is thus provided a remote communication terminal for verified communication, the terminal comprising:

a sound input,

a password encoder connected to said sound input for encoding a voice password identified from said sound input to provide said password with resilience for transmission in a noisy channel, and

a password output connected to said password encoder for sending said resiliently encoded password over a channel to an authenticator.

A preferred embodiment comprises a sound output connected to said sound input for sending sound data over a channel to a communication destination.
Preferably, said password output is operable to send said resiliently encoded password using a first communication protocol and said sound output is operable to send said sound data using a second communication protocol.

Preferably, said password output is operable to send said resiliently encoded password using a first communication channel and said sound output is operable to send said sound data using a second communication channel.

Preferably, said first communication channel uses a first communication protocol and said second communication channel uses a second communication protocol.

Preferably, said password encoder comprises a digitizer.
Preferably, said password encoder comprises a channel encoder.
Preferably, said channel encoder comprises a cyclic redundancy check encoder.
Alternatively or additionally said channel encoder comprises a Huffman encoder.

Alternatively or additionally said channel encoder comprises a turbo encoder.
Alternatively or additionally said channel encoder comprises a block encoder.

Preferably, said password encoder further comprises a compressor for compressing said digitized password.

Preferably, said password encoder further comprises an encryptor for encrypting said password.

Preferably, said first communication channel is a digital communication channel and said second communication channel is an analog communication channel.

Preferably, said first communication channel is a cellular digital communication channel.

Preferably, said first communication protocol is the Wireless Application Protocol (WAP).

Preferably, said second communication channel is GSM.

Preferably, said second communication channel is a third generation cellular telephony channel.
According to a second aspect of the present invention, there is provided remote authentication apparatus for authenticating a voice message comprising a separately transmitted channel encoded password and message body, the apparatus comprising:

- a password receiver for receiving said channel encoded password,
- a password decoder for decoding said password,
- a password authenticator for authenticating said decoded password, and
- and a message body receiver for receiving said message body for processing in accordance with said authentication.

Preferably, said password receiver is operable to receive said channel encoded password using a first communication protocol and said message body receiver is operable to receive said sound data using a second communication protocol.

Preferably, said password receiver is operable to receive said resiliently encoded password using a first communication channel and said message body receiver is operable to receive said sound data using a second communication channel.

Preferably, said first communication channel uses a first communication protocol and said second communication channel uses a second communication protocol.

Preferably, said password receiver comprises a digital to analog converter.

Preferably, said password decoder comprises a channel decoder.

Preferably, said channel decoder comprises a cyclic redundancy check decoder.

Alternatively or additionally said channel decoder comprises a Huffman decoder.

Alternatively or additionally said channel decoder comprises a turbo decoder.

Alternatively or additionally said channel decoder comprises a block decoder.

Alternatively or additionally said channel decoder comprises a Viterbi decoder.

Preferably, channel encoded password is receivable in compressed format and said password decoder comprises a decompressor for decompressing said digitized password.

Preferably, said channel encoded password is receivable in encrypted format and said password decoder comprises a decryptor for decrypting said digitized password.
Preferably, said first communication channel is a digital communication channel and said second communication channel is an analog communication channel.

Preferably, said first communication channel is a cellular digital communication channel.

Preferably, said first communication protocol is the Wireless Application Protocol (WAP).

Preferably, said second communication channel is GSM.

According to a third aspect of the present invention there is provided remote authentication apparatus wherein said password authenticator comprises a stored sample password and a distance measurer, wherein said distance measurer is operable to measure a distance between said received password and said stored sample password, and wherein said authenticator further comprises a comparator for comparing said measured distance against a threshold, thereby to determine whether said received password is the same as said stored password.

According to a fourth aspect of the present invention there is provided remote authentication apparatus for authenticating a voice message comprising a separately transmitted channel encoded authentication phrase and message body, the apparatus comprising:

an authentication phrase receiver for receiving said channel encoded password,

an authentication phrase decoder for decoding said authentication phrase,

an authenticator for authenticating said decoded authentication phrase by determining that said authentication phrase contains an expected voiceprint, and

a message body receiver for receiving said message body for processing in accordance with said authentication.

According to a fifth aspect of the present invention there is provided a method of obtaining or providing a password for remote authorization comprising:

connecting to a remote server using a first level of channel protection,

receiving a vocal password from a user, and

encoding said vocal password for transmission using a second level of channel protection, wherein said second level of channel protection is higher than said first level of channel protection.
Brief Description of the Drawings

For a better understanding of the invention and to show how the same may be carried into effect, reference will now be made, purely by way of example, to the accompanying drawings.

With specific reference now to the drawings in detail, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of the preferred embodiments of the present invention only, and are presented in the cause of providing what is believed to be the most useful and readily understood description of the principles and conceptual aspects of the invention. In this regard, no attempt is made to show structural details of the invention in more detail than is necessary for a fundamental understanding of the invention, the description taken with the drawings making apparent to those skilled in the art how the several forms of the invention may be embodied in practice. In the accompanying drawings:

Fig. 1 is a simplified diagram of a system for reliable voice-based authorization according to a first embodiment of the present invention,

Fig. 2 is a simplified block diagram of the communication device of Fig. 1,

Fig. 3 is a simplified block diagram of the receiving location of Fig. 1, and

Fig. 4 is a simplified flow diagram of a communication procedure involving voice authorization.

Description of the Preferred Embodiments

Before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and the arrangement of the components set forth in the following description or illustrated in the drawings. The invention is applicable to other embodiments or of being practiced or carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein is for the purpose of description and should not be regarded as limiting.

Reference is now made to Fig. 1, which is a simplified diagram of a system according to a first embodiment of the present invention. In the system of Fig. 1, a
communication device 10 is located at a sending location 12. The communication
device comprises a client module 14 which comprises the standard functionality of the
communication device 10, such as GSM cellular telephony functionality. In addition
there is provided a password processor 16 which is operable to identify password or
other authentication material of a communication and process the password for secure
transfer separately from the message body. As will be explained in more detail below,
the password may be transferred either over a different channel from the message body
or over the same channel but in a more secure manner. For example third generation
mobile telephony standards support different levels of error protection over a single
channel.

Fig. 1 shows an embodiment in which two separate channels, channel A and
channel B are used. Channel A is used for transferring the message body and channel
B is for transferring the password or other authentication information. The channels
are standard communication channels, which may involve radio or cellular links at
various stages and are liable to add noise or introduce distortion into any signal
transferred. The communication is preferably set up on the two channels
simultaneously. In one preferred embodiment one of the channels is a voice channel
and the other channel is a data channel. In general, data channels have higher levels of
protection against noise and distortion as opposed to voice channels since data-based
applications generally require close to perfect data transfer.

A receiving location 18 preferably comprises two servers, a communication
server 20 and an authentication server 22. The communication server 20 processes the
body of the communication, for example it carries out an interactive process or obtains
information for a user. The communication server 20 may be a server that holds bank
account or other personal information of a user or may be an e-commerce site or any
other example of a server for which reliable authentication may be required.

The authentication server receives the password and, as will be explained
below, decodes it to remove noise and distortion. The decoded password is then used
in a process involving voice recognition and authentication to identify either the
password or the user, again as will be explained below. Provided that authentication is
achieved then an authorization is provided to communication server 20.
Communication server 20 may require the authorization to permit data access or to permit a transaction or for any other purpose to obtain positive identity of a user.

Reference is now made to Fig. 2, which is a simplified block diagram of the communication device 10 of Fig. 1. Parts that are identical to those shown above are given the same reference numerals and are not referred to again except as necessary for an understanding of the present embodiment. The client module 14 comprises a sound input 30 which may be a standard microphone. A message body processor 32 processes the entirety of a message in the normal way, for example as a GSM-based cellular telephone call and the message is output via a standard output 34 for transmission.

At some stage in a communication requiring authorization, the user is asked to speak a password or authentication phrase. A password extractor 36 is able to extract the part of the sound input data comprising the password for processing separately from the rest of the message. It is noted that the password bearing part may be cut, that is to say removed, from the message body, or it may simply be copied so that the message body remains intact.

The skilled person will be able to provide a number of ways in which the password extractor may extract the password. One way is for the user to press on a button at the time he is saying the password. Another possibility is for the authentication server 22 to send a control signal to the device 10 at the time that it requests the password, which control signal switches on the password extractor for a predetermined amount of time. In selecting the amount of time that the password extractor is switched on it is noted that the data extracted should preferably include the entire password but it is less critical as to whether it contains only the password or whether it contains other parts of the message in additional since the authentication part of the password authorization process is able to recognize the password from amongst other data.

The extracted password, or voice stream containing the password or authentication phrase, is then sent to a password encoder 38. The password encoder preferably comprises an A/D converter for digitizing the voice stream. Alternatively digitization may be incorporated into the sound input 30 for digitization of the
message body and password before they are separated. The password encoder further
comprises a channel encoder 42 for encoding the password in a form suitable for
robust transmission over a noisy channel. Encoding may involve any known channel
encoding scheme, for example CRC codes of various kinds including trellis codes,
block codes, turbo codes and the like. Many channel encoding schemes allow
selectable levels of protection. Generally, the higher the level of protection the higher
the bandwidth required by the transmission and thus many transmission systems try to
limit the level of protection to the minimum necessary for successful receipt. In
particular voice channels are generally given a relatively low level of protection since
even with a high level of distortion, human voice is recognizable to the ear of the
receiver. However the same does not apply to automatic voice processing and thus it
is desirable to provide the password part of the message with a level of protection
closer to that given to digital data, where incorrect receipt of even a single bit can lead
to havoc in interpreting the data.

Thus, channel encoder 42 preferably provides a high level of channel protection
to the password and the password is sent as protected digitized data. In preferred
embodiments the password encoder 38 further comprises an encryptor 44 for
encrypting the password. The password may be sent as a separately identifiable unit
and an eavesdropper able to identify the unit is able to copy it and hack into the
system. Thus it is preferable that the password-bearing data unit is encrypted in such a
way that simple copying would not put an eavesdropper in possession of the password.
For example the password may be encrypted such that successive encryptions of the
same password are never the same.

The password encoder 38 also preferably comprises a data compressor 46. The
data compressor may use any data compression scheme in order to compress the
extracted signal bearing the password. Compression schemes include vocoder-based
schemes which are specifically intended for compression of voice data. In using such
compression schemes the skilled person should preferably bear in mind the need to
maintain voice quality. One way of maintaining voice quality is to use a vocoder
scheme for voice compression that corresponds to the voice recognition and
authentication technology used by the authenticator, thereby retaining all the voice
information that is used in the recognition part of the authentication process.

The processed signal bearing the password is then sent to a password output 48. The password output may send data over the same channel as the message body but more robustly encoded as a result of the channel encoding above, or it may send the data over a different channel. For example many current mobile telephones are enabled for data communications using such schemes as WAP as well as voice communication over standard GSM. Thus the message body may be transmitted in the normal way over the voice channel and the password processor may simply make use of the standard WAP functionality for encoding and output.

Reference is now made to Fig. 3, which is a simplified block diagram of the receiving location 20 of Fig. 1. Parts that are identical to those shown above are given the same reference numerals and are not referred to again except as necessary for an understanding of the present embodiment. A communication server 18 comprises a message body receiver 50 for receiving the main body of the message. A message body processor 52 carries out a procedure that requires authorization, the procedure itself based on interaction with the main body of the message.

The authentication server 22 comprises an authentication phrase receiver 54 for receiving the channel encoded authentication phrase or password or message segment containing the same, hereinafter referred to as the password. The authentication phrase receiver 54 receives the password and buffers it as necessary. The password is passed to an authentication phrase decoder 56 where channel decoding, decompression and decryption are preferably carried out by channel decoding unit 58, decryptor 60 and decompressor 62 so that the original password phrase is recovered.

A D/A converter 64 is also shown. If the voice recognition and authentication apparatus is analog-based then the password is reconverted into analog form before processing, but if the voice recognition and authentication technology is digitally based then the D/A converter may be dispensed with.

Furthermore, if voice compression at the password processor is based on a vocoder system that corresponds to the voice recognition and authentication technology then decompressor 62 may also be dispensed with.
The output of the authentication phrase decoder is passed to authenticator 66. Authenticator 66 may comprise voice recognition functionality intended to match a received password to a template stored in an associated sample memory 68. The authenticator uses voice analysis to produce a reduced form of the received password which is then matched against a sample using distance measuring techniques. If the distance between the template and the spoken password is below a predetermined threshold then authorization is given, otherwise the user is requested to repeat the password. Preferably after a predetermined number of unsuccessful repetitions the session is terminated.

The template is a recorded and processed sample of the user speaking the password. The distance between the spoken password and the template is generally speaker dependent in that a different user speaking the same password will often achieve a greater distance from the template than the original user. Thus, suitable setting of the predetermined threshold may effectively make the password user specific, meaning that another user, even if he/she discovers what the password is, will not be able to reproduce it to the satisfaction of the authenticator.

In an alternative embodiment, the authenticator obtains a voice print. A voice print comprises characteristics of the user’s voice which are entirely speaker dependent and are independent of the words spoken. Thus the user need not speak a predetermined password but rather speaks a phrase of sufficient length to enable voice print information to be extracted. The user is either identified or not and authorization issued or denied accordingly.

Reference is now made to Fig. 4, which is a simplified flow chart showing a procedure for setting up a process requiring authorization according to an embodiment of the present invention. The flow chart shows stages divided into those that occur at the user location and those that occur at the server location.

During process setup, a user sends a unique identifier which serves as a user name. A request for authentication is then sent to the user via either of the channels involved in the communication. The user responds by speaking the password or an authentication phrase which is extracted, as explained above, by the password extractor. The password is optionally compressed and encrypted and then is channel
encoded for a WAP channel. The password is sent via the WAP channel and decoded as necessary at the authorization server. The password is used to verify the identity of the user and authorization is granted or denied. The communication device is prompted as to whether authentication is successful and authorization has been granted. If authorization is not granted then the user may be prompted to repeat the password up to a predetermined number of times until a final denial is issued and the communication session is terminated.

In the event of successful authorization, the process requiring authorization is begun.

There is thus provided a system that permits reliable voice-based authorization for processes and activities carried out over noisy and distorting communication channels.

It is appreciated that certain features of the invention, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather the scope of the present invention is defined by the appended claims and includes both combinations and subcombinations of the various features described hereinabove as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description.
Claims

1. A remote communication terminal for verified communication, the terminal comprising:
   a sound input,
   a password encoder connected to said sound input for encoding a voice password identified from said sound input to provide said password with resilience for transmission in a noisy channel, and
   a password output connected to said password encoder for sending said resiliently encoded password over a channel to an authenticator.

2. A remote communication terminal according to claim 1, further comprising a sound output connected to said sound input for sending sound data over a channel to a communication destination.

3. A remote communication terminal according to claim 2, wherein said password output is operable to send said resiliently encoded password using a first communication protocol and said sound output is operable to send said sound data using a second communication protocol.

4. A remote communication terminal according to claim 2, wherein said password output is operable to send said resiliently encoded password using a first communication channel and said sound output is operable to send said sound data using a second communication channel.

5. A remote communication terminal according to claim 4, wherein said first communication channel uses a first communication protocol and said second communication channel uses a second communication protocol.

6. A remote communication terminal according to claim 1, wherein said password encoder comprises a digitizer.
7. A remote communication terminal according to claim 1, wherein said password encoder comprises a channel encoder.

8. A remote communication terminal according to claim 7, wherein said channel encoder comprises a cyclic redundancy check encoder.

9. A remote communication terminal according to claim 7, wherein said channel encoder comprises a Huffman encoder.

10. A remote communication terminal according to claim 7, wherein said channel encoder comprises a turbo encoder.

11. A remote communication terminal according to claim 7, wherein said channel encoder comprises a block encoder.

12. A remote communication terminal according to claim 6, wherein said password encoder further comprises a compressor for compressing said digitized password.

13. A remote communication terminal according to claim 6, wherein said password encoder further comprises an encryptor for encrypting said password.

14. A remote communication terminal according to claim 5, wherein said first communication channel is a digital communication channel and said second communication channel is an analog communication channel.

15. A remote communication terminal according to claim 5, wherein said first communication channel is a cellular digital communication channel.

16. A remote communication terminal according to claim 5, wherein said first communication protocol is the Wireless Application Protocol (WAP).
17. A remote communication terminal according to claim 5, wherein said second communication channel is GSM.

18. A remote communication terminal according to claim 5, wherein said second communication channel is a third generation cellular telephony channel.

19. Remote authentication apparatus for authenticating a voice message comprising a separately transmitted channel encoded password and message body, the apparatus comprising:
   a password receiver for receiving said channel encoded password,
   a password decoder for decoding said password,
   a password authenticator for authenticating said decoded password, and
   and a message body receiver for receiving said message body for processing in accordance with said authentication.

20. Remote authentication apparatus according to claim 19, wherein said password receiver is operable to receive said channel encoded password using a first communication protocol and said message body receiver is operable to receive said sound data using a second communication protocol.

21. Remote authentication apparatus according to claim 19, wherein said password receiver is operable to receive said resiliently encoded password using a first communication channel and said message body receiver is operable to receive said sound data using a second communication channel.

22. Remote authentication apparatus according to claim 21, wherein said first communication channel uses a first communication protocol and said second communication channel uses a second communication protocol.
23. Remote authentication apparatus according to claim 19, wherein said password receiver comprises a digital to analog converter.

24. Remote authentication apparatus according to claim 19, wherein said password decoder comprises a channel decoder.

25. Remote authentication apparatus according to claim 24, wherein said channel decoder comprises a cyclic redundancy check decoder.

26. Remote authentication apparatus according to claim 24, wherein said channel decoder comprises a Huffman decoder.

27. Remote authentication apparatus according to claim 24, wherein said channel decoder comprises a turbo decoder.

28. Remote authentication apparatus according to claim 24, wherein said channel decoder comprises a block decoder.

29. Remote authentication apparatus according to claim 24, wherein said channel decoder comprises a Viterbi decoder.

30. Remote authentication apparatus according to claim 19, said channel encoded password being receivable in compressed format and wherein said password decoder comprises a decompressor for decompressing said digitized password.

31. Remote authentication apparatus according to claim 19, said channel encoded password being receivable in encrypted format and wherein said password decoder comprises a decryptor for decrypting said digitized password.
32. Remote authentication apparatus according to claim 22, wherein said first communication channel is a digital communication channel and said second communication channel is an analog communication channel.

33. Remote authentication apparatus according to claim 22, wherein said first communication channel is a cellular digital communication channel.

34. Remote authentication apparatus according to claim 22, wherein said first communication protocol is the Wireless Application Protocol (WAP).

35. Remote authentication apparatus according to claim 22, wherein said second communication channel is GSM.

36. Remote authentication apparatus wherein said password authenticator comprises a stored sample password and a distance measurer, wherein said distance measurer is operable to measure a distance between said received password and said stored sample password, and wherein said authenticator further comprises a comparator for comparing said measured distance against a threshold, thereby to determine whether said received password is the same as said stored password.

37. Remote authentication apparatus for authenticating a voice message comprising a separately transmitted channel encoded authentication phrase and message body, the apparatus comprising:
   an authentication phrase receiver for receiving said channel encoded password,
   an authentication phrase decoder for decoding said authentication phrase,
   an authenticator for authenticating said decoded authentication phrase by determining that said authentication phrase contains an expected voiceprint, and
   a message body receiver for receiving said message body for processing in accordance with said authentication.
38. Method of providing a password for remote authorization comprising:
   connecting to a remote server using a first level of channel protection,
   receiving a vocal password from a user, and
   encoding said vocal password for transmission using a second level of channel
   protection, wherein said second level of channel protection is higher than said first
   level of channel protection.
Fig. 1

Sending Location

Communication device

Password Processor

Client Module

Receiving Location

Authentication Facility

Authentication Server

Communication Server

Communication link A

Communication link B

12

18

16

10

22

20

SUBSTITUTE SHEET (RULE 26)
Sending location

User sends unique identifier, via GSM

Receiving location

request for authentication using either GSM or WAP

User prompted to speak vocal password

User speaks vocal password which is sent to password extractor

Captured vocal password optionally compressed and/or encrypted

Captured vocal password sent using WAP to authentication server

Authentication facility verifies the users identity

Communication device is prompted as to whether authentication is successful. Upon denial, session is terminated

Communication via WAP or GSM

Fig. 4