Abstract:

Title: METHOD AND SYSTEM FOR SECURE DATA TRANSFER

A method and system for transferring data between a communication device and a server in a secure manner is disclosed. The data sequences are transferred as dual tone multi-frequency tones between the communication device and the server. The system prevents the deciphering of data by a third party. The third party receives information which is a combination of data transmitted by the user of the communication device and random information generated by the server.
FIELD OF THE INVENTION

The present invention relates to a system and a method for transferring data between a communication device and a server. More particularly, the invention relates to a method for securely transferring data as dual tone multi-frequency tones between a communication device and a server.

DEFINITIONS

Caller: A person using a communication device to transfer data to a secure system.

Third Party: A person who tries to decipher the data being transmitted by the caller.

BACKGROUND

The data transferred over a communication network may be critical information such as the credit card numbers and the bank account numbers. The data may be in the form of wave signals of different amplitudes and frequencies such as Dual Tone Multi-Frequency (DTMF) signals and voice signals.

For the transfer of data, a typical communication network includes two nodes that may be sending and receiving data simultaneously over a communication channel. Examples of the communication network include, but are not limited to, mobile telecommunication network like Global System for Mobile communications (GSM) network, and the Internet.

Security has been an important issue of concern in the transfer of data over the communication channel. Security concerns arise when a third party attempts to access the data being transferred. Any data transfer over an insecure communication channel is likely to be accessed and interpreted by the third party which may further lead to misuse of such data by the third party. Multiple
techniques have been developed to ensure secure and uninterrupted transfer of data over the communication channel.

Such a system and a method was disclosed in US Patent 6012144, titled "Transaction security method and apparatus", published on January 4, 2000. The patent discloses a method and a system to ensure secure data transfer by prompting the user to send the data in parts. The method requires the user to send out one part of her credit card number over a communication channel. Thereafter, an Interactive Voice Response System (IVRS) is initiated which requires the user to enter the remaining part of her credit card number. However, the method has a disadvantage that a third party may still access the data transferred in parts. Also, this mechanism mandates the use of at least two different communication channels to make a transaction, which may not be available to the user at all times.

Similarly, another method and system includes converting the DTMF signals and voice signals into bytes and encrypting the bytes before sending the data over the communication channel. However, such a method requires sophisticated and expensive devices for encrypting the data.

In light of the above mentioned limitations, there is a need for a method and system of transferring data that is sent in the form of dual tone multi-frequency signals over a telephonic communication channel. Further, the method should not require any additional devices at each communicating end for encrypting the data before sending it over the communication channel. Moreover, the method should also prevent the data from being accessed and deciphered by the third party.

SUMMARY OF THE INVENTION

According to an embodiment of the invention, a method of making a secure data transfer between a caller and a secure system over a
communication channel is disclosed. A third party has access to the data being transferred between the caller and the secure system. The method includes receiving a portion of a data sequence from the caller. The data sequence is associated with a pre-defined pattern. Further, the method includes generating a random data sequence based on the pre-defined pattern. The method also includes combining the portion of the data sequence and the random data sequence based on the pre-defined pattern. Furthermore, the method includes communicating the combined sequence to the third party upon an attempt by the third party to access the portion of the data sequence.

According to another embodiment of the invention, a method of making a secure data transfer between a caller and a secure system over a communication channel is disclosed. The transfer of data is through dual tone multi-frequency (DTMF) tones and a third party has access to the data being transmitted between the caller and the secure system. The method includes receiving a data sequence being transferred as DTMF tones from the caller over the communication channel. The data sequence is associated with a pre-defined pattern. Further, the method includes receiving a random data sequence as DTMF tones from the secure system. The method also includes combining the data sequence and the random data sequence based on the pre-defined pattern. Furthermore, the method includes communicating the combined sequence to the third party when the third party attempts to access the data sequence.

According to yet another embodiment of the invention, a system for making a secure data transfer between a caller and a secure system over a communication channel is disclosed. The data is being transmitted as DTMF tones and a third party has access to the data being transmitted between the caller and the secure system. The system includes a waveform recorder for measuring characteristics of the DTMF tones sent by the caller. The characteristics may include amplitude, duration and frequency of the DTMF tones. The system also includes a DTMF mask generator for generating a
random string of numbers based on a pre-defined pattern. Further, the system includes a DTMF tone generator for converting the random string to a random data sequence based on the characteristics of the DTMF tones sent by the caller. The random data sequence is generated as dual tone multi-frequency tones. Furthermore, the system includes a conferencing system such as a Private Branch Exchange (PBX) to receive a data sequence as dual tone multi-frequency tones from the caller over the communication channel. The data sequence is associated with a pre-defined pattern. The conferencing system is also configured to combine the data sequence and the random data sequence based on the pre-defined pattern. Further, the conferencing system is configured to communicate the combined sequence to the third party upon an attempt by the third party to access the data sequence.

**BRIEF DESCRIPTION OF THE DRAWINGS**

FIG. 1 is a schematic illustrating the environment for the invention; FIG. 2 is a flow diagram illustrating a method for secure data transfer, in accordance with an embodiment of the invention; FIG. 3 is a schematic illustrating a secure system, in accordance with an embodiment of the invention; and FIG. 4 is a schematic illustrating a server, in accordance with an embodiment of the invention.

**DETAILED DESCRIPTION**

In the following description, for the purposes of explanation, specific details are set forth in order to provide a thorough understanding. It will be apparent, however, to one skilled in the art that the present invention may be practiced without these specific details. Various aspects and features of example embodiments of the invention are described in more detail hereinafter. In other instances, well known features have not been described so as not to obscure the invention.
FIG. 1 is a schematic illustrating the environment 100 for the invention. The environment 100 includes a caller 102, a secure system 104, and a third party 106. Caller 102 is connected to secure system 104 via a communication network 108. According to an embodiment, caller 102 initiates a call to third party 106 by using communication devices such as a mobile phone, a smart phone, a landline phone or a Personal Digital Assistant (PDA).

Third party 106 initiates the call with caller 102. The call is forwarded to a server (described in FIG. 4) of secure system 104 when a secure data exchange needs to be done between caller 102 and secure system 104. Hence, caller 102, the server, and third party 106 are in a conference call. According to an embodiment, the forwarding may be triggered by third party 106. Further, third party 106 may be an operator at a call centre. Caller 102 transfers a data sequence to secure system 104 when caller 102 is prompted by secure system 104 to enter the data sequence. The data sequence is transferred over a communication channel as dual tone multi-frequency (DTMF) tones. According to an embodiment, third party 106 may attempt to access and interpret the data sequence transferred by caller 102 to secure system 104 by tapping into secure system 104. Examples of the communication channel include, but are not limited to a Global System for Mobile Communication (GSM) communication channel and a Code Division Multiple Access (CDMA) communication channel.

FIG. 2 is a flow diagram illustrating a method for secure data transfer, in accordance with an embodiment of the invention. The method of FIG. 2 is executed when a call is initiated by caller 102 to third party 106. Thereafter, the call is forwarded by third party 106 to secure system 104 and caller 102 is prompted by secure system 104 to enter a data sequence. The data sequence may correspond to any sensitive information such as, credit card number, debit card number, automated teller machine (ATM) pin, bank account number or any number that needs to be transferred securely. For example, in a bidding system,
the bid amount can be transferred securely by a bidder through secure system 104.

At step 202, secure system 104 receives a portion of the data sequence from caller 102. The data sequence is associated with a pre-defined pattern. The pre-defined pattern may include rules that correspond to, for example, a credit card number, a debit card number, an ATM pin, a bank account number or any number that needs to be transferred securely. An example of the pre-defined pattern may be that a credit card number consists of 16 digits. An example of the rule may be that a VISA credit card number begins with the digit 4. Another example of the rule may be that a MasterCard credit card number begin with the digit 5. At step 204, secure system 104 generates a random data sequence based on the pre-defined pattern. At step 206, the portion of the data sequence received and the generated random data sequence are combined based on the pre-defined pattern. The portion of the data sequence received may be the first four digits of the credit card number. According to an embodiment, third party 106 may attempt to access and interpret the data sequence entered by caller 102. At step 208, the combined sequence is communicated to third party 106 when third party 106 attempts to access the data sequence from secure system 104. The secure system 104 is described in detail in FIG. 3.

FIG. 3 is a schematic illustrating secure system 104, in accordance with an embodiment of the invention. Secure system 104 includes a conferencing system 302 and a server 304. Conferencing system 302 establishes connections between caller 102 and third party 106. Also, conferencing system 302 is connected to server 304. According to an embodiment, caller 102, server 304 and third party 106 are in a conference call. Conferencing system 302 transfers the data sequence entered by caller 102 to server 304. The data sequence being transferred by caller 102 through conferencing system 302 is available to server 304 and third party 106. Similarly, data transferred by server 304 or third party 106 is available to the other two parties.
According to an embodiment, the data sequence transferred by caller 102 is received by conferencing system 302 as DTMF tones. The data sequence is associated with pre-defined patterns such as a credit card number, bank account number, an ATM pin or any number that needs to be transferred securely. The pre-defined pattern may include rules corresponding to the credit card number, the bank account number, etc. An example of the pre-defined pattern may be that a credit card number consists of 16 digits. An example of the rule may be that a VISA credit card number begins with the digit 4. Another example of the rule may be that a MasterCard credit card number begin with the digit 5. Server 304 generates a random data sequence based on the pre-defined pattern of the portion of the data sequence received from caller 102 and sends it to conferencing system 302. Thereafter, the data sequence and the random data sequence are combined by conferencing system 302 and communicated to third party 106 whenever it tries to intercept the portion of the data sequence.

The above mentioned method can be described in conjunction with the following example. Suppose server 304 prompts caller 102 to enter her 16-digit VISA credit card number. As caller 102 enters her credit card number, server 304 associates the portion of data sequence received, say 1234, with a pre-defined pattern, such as VISA credit card number. Thereafter, server 304 generates a random data sequence, such as 5678, based on the pre-defined pattern. According to an embodiment, the pre-defined pattern may include one or more rules. The random data sequence 5678 conforms to the rules of VISA credit card numbers stored in server 304. Conferencing system 302 receives the random data sequence 5678 from server 304. Thereafter, conferencing system 302 combines the portion of data sequence 1234 and the random data sequence 5678. The combined sequence is a random sequence that is generated based on the time instant at which the digits of the data sequence and the random data sequence are received by conferencing system 302. The combined sequence may, for an embodiment, be 125364. Hence, third party 106 intending to
intercept and interpret the VISA credit card data sequence 1234 entered by caller 102 will receive the combined data sequence 125364 instead of 1234. This prevents the misuse of the critical information sent by caller 102 by third party 106. The server 304 is explained in detail in FIG. 4.

FIG. 4 is a schematic illustrating server 304, in accordance with an embodiment of the invention. Server 304 includes an Interactive Voice Response System (IVRS), an application 406, a DTMF mask generator 408, a configurator 410 and a DTMF tone generator 412. The IVRS includes a telephony device driver 402, a Dual Tone Multi-frequency (DTMF) interpreter 404, a waveform recorder 414 and a waveform playback module 416.

Caller 102 initiates a call with third party 106. The call is forwarded to server 304 when secure data is to be exchanged between caller 102 and server 304. According to an embodiment, the call is forwarded by third party 106 to server 304. Thereafter, application 406 prompts caller 102 to enter a data sequence. The data sequence may be DTMF tones corresponding to domains such as a credit card number, a debit card number, a bank account number or an ATM pin. Telephony device driver 402 receives a portion of data sequence as DTMF tones and sends them to the DTMF interpreter 404. DTMF interpreter 404 decodes the DTMF tones into corresponding digits of the data sequence. Application 406, after prompting the user to enter the data sequence and before receiving the digits corresponding to the data sequence, informs DTMF mask generator 408 of the domain associated with the data sequence. DTMF mask generator 408 picks up a pre-defined pattern associated with the domain from configurator 410.

Configurator 410 is a database that stores pre-defined patterns associated with different data sequences. Examples of the pre-defined patterns may include rules corresponding to VISA 16-digit credit card number, VISA debit card number, VISA bank account number, etc. Application 406 receives the digits and
verifies certain information related to the portion of the data sequence received. According to an embodiment, application 406 verifies information such as checksum associated with the digits of the data sequence. Thereafter, DTMF mask generator 408 generates random digits based on the pre-defined pattern.

The random digits generated by DTMF mask generator 408 are sent to DTMF tone generator 412. DTMF tone generator 412 receives the random digits generated by DTMF mask generator 408 and also certain characteristics measured by waveform recorder 414. Thereafter, DTMF tone generator 412 generates a random data sequence comprising the random digits in the form of DTMF tones. According to an embodiment, the characteristics measured by waveform recorder 414 may include amplitude, duration, length and frequency of the DTMF tones corresponding to the portion of the data sequence entered by caller 102. The generated DTMF tones have their amplitude and length close to the values measured by waveform recorder 414, i.e., the random data sequence has tones whose amplitude and length are close to that of the data sequence's tones. Thereafter, waveform playback module 416 plays the random data sequence to telephony device driver 402. Telephony device driver 402 relays the random data sequence to conferencing system 302. Conferencing system 302 combines the data sequence sent by caller 102 and random data sequence sent by server 304. Further, conferencing system 302 transmits the combined sequence to third party 106 when third party 106 attempts to obtain data sequence sent by caller 102.

The above mentioned method can be explained in conjunction with the following example. Consider a situation where the caller 102 enters a portion of her VISA credit card data sequence 1234. Conferencing system 302 directs the portion of the data sequence 1234 which is in the form of DTMF tones to telephony device driver 402. Telephony device driver 402 sends the DTMF tones to DTMF interpreter 404. Further, DTMF interpreter 404 converts the DTMF tones into actual digits 1234. Application 406 before receiving the portion of the
data sequence as digits informs DTMF mask generator 408 of the domain 
associated with the data sequence i.e. the data sequence corresponds to a credit 
card number. DTMF mask generator 408 picks up the pre-defined pattern 
 corresponding to the credit card number from configurator 410. The pre-defined 
pattern includes rules associated with the VISA credit card number. Application 
406 receives the portion of the data sequence 1234. Thereafter, DTMF mask 
generator 408 generates random digits based on the pre-defined pattern. 
Application 406 also verifies the validity of the data sequence 1234. Thereafter, 
random numbers 5678 are generated which will conform to the pre-defined 
pattern. For instance, the number of digits in the random sequence generated is 
four, which is same as the incoming data sequence. The DTMF tones 
corresponding to this random data sequence are subsequently sent to the 
waveform playback module 416. Further, waveform playback module 416 relays 
the DTMF tones to the telephony device driver 402. Telephony device driver 402 
transmits the DTMF tones to the conferencing system 302.

It will be apparent to a person skilled in the art that the conferencing 
system may have a plurality of users engaged in a conference call. For example, 
in a bidding system, multiple bidders may bid an amount over a conference call. 
The bidders enter the bid amount when prompted by the server. All the bidders 
have access to the bid amounts entered by the other bidders. The secure system 
prevents any bidder from interpreting the bid amount entered by another bidder, 
by combining the bid amount entered by the bidder with a random sequence. 
Thereafter the combined sequence is communicated to other bidders. Hence, the 
bid amount entered by the bidder can not be interpreted by another bidder.

Various embodiments of the invention provide methods and system for 
secure data transfer between a caller and a server in a communication network.
The data is transferred in the form of DTMF signals over the communication 
channel. The method does not require the use of any extra device located with 
the caller or the third party for encrypting the data before sending it over the
coincident situation channel. Further, the method transfers random data to a third party whenever any third party tries to access the data being transferred. Hence, interpretation of actual data by the third party is prevented.

While example embodiments of the invention have been illustrated and described, it will be clear that the invention is not limited to these embodiments only. Numerous modifications, changes, variations, substitutions and equivalents will be apparent to those skilled in the art without departing from the spirit and scope of the invention as described in the claims.
1. A method of making a secure data transfer between a caller and a server, the data being transferred over a communication channel, a third party having access to the data being transferred over the communication channel, the method comprising:
   a. receiving a portion of a data sequence from the caller over the communication channel, the data sequence being associated with a pre-defined pattern;
   b. generating a random data sequence based on the pre-defined pattern;
   c. combining the portion of the data sequence and the random data sequence based on the pre-defined pattern; and
   d. communicating the combined sequence to the third party upon an attempt by the third party to access the portion of the data sequence.

2. The method of claim 1, wherein the portion of the data sequence is received as dual tone multi-frequency tones.

3. The method of claim 1, wherein the random data sequence is generated as dual tone multi-frequency tones.

4. The method of claim 1, wherein the communication channel is at least one of a global system for mobile communication channel, a voice over internet protocol communication channel, a regular analog communication channel and a code division multiple access communication channel.

5. A method of making a secure data transfer between a caller and a server, the data being transferred over a communication channel as dual tone multi-frequency tones, a third party having access to the data being transferred over the communication channel, the method comprising:
a. receiving a portion of a data sequence as dual tone multi-frequency tones from the caller over the communication channel, the portion of the data sequence being associated with a pre-defined pattern;
b. receiving a random data sequence as dual tone multi-frequency tones, the random data sequence being based on the pre-defined pattern;
c. combining the portion of the data sequence and the random data sequence based on the pre-defined pattern; and
d. communicating the combined sequence to the third party upon an attempt by the third party to access the data sequence.

6. The method of claim 5 wherein the communication channel is at least one of a global system for mobile communication channel, a voice over internet protocol communication channel, a regular analog communication channel and a code division multiple access communication channel.

7. A system for making a secure data transfer between a caller and a server, the data being transferred over a communication channel as dual tone multi-frequency tones, a third party having access to the data being transferred over the communication channel, the system comprising:

a. a waveform recorder for measuring characteristics of the dual tone multi-frequency tones;
b. a dual tone multi-frequency mask generator for generating a random string based on a pre-defined pattern;
c. a dual tone multi-frequency tone generator for converting the random string to a random data sequence based on the characteristics of the dual tone multi-frequency tones, wherein the random data sequence is generated as dual tone multi-frequency tones; and
d. a conferencing system configured to:
i. receive a portion of a data sequence as dual tone multi-frequency tones from the caller over the communication channel, the portion of the data sequence being associated with the pre-defined pattern;

ii. combine the portion of the data sequence and the random data sequence based on the pre-defined pattern; and

iii. communicate the combined sequence to the third party upon an attempt by the third party to access the data sequence.

8. The system of claim 7 further comprising a configurator for storing a plurality of pre-defined patterns.

9. The system of claim 7 further comprising a DTMF interpreter for converting the dual tone multi-frequency tones to numbers.

10. The system of claim 7, wherein the communication channel is at least one of a global system for mobile communication channel, a voice over internet protocol communication channel, a regular analog communication channel and a code division multiple access communication channel.
FIG. 1
Start

Secure system receives data sequence from caller as DTMF tones

Secure system generates random data sequence

Secure system combines random data sequence and data sequence

Secure system communicates combination of data sequence and random data sequence to third party

Stop

FIG. 2
FIG. 4