AUTHENTICATION OF A SUBSCRIBER STATION

The invention relates to a method for identifying authentication messages that have been generated by external attackers. According to the method, when a subscriber station receives an authentication input (2-4), it compares (2-5) the received authentication input with information of earlier-received authentication inputs. The subscriber station evaluates (2-5) the randomness of the received authentication input utilizing the information of earlier-received authentication inputs. If the subscriber station finds the new input random, it responds (2-6) to it in a usual manner. If the subscriber station finds the input non-random it concludes that the input has been generated by an external attacker trying to crack the secret key of the subscriber station. In such a case the subscriber station may lock the authentication process and/or it may generate a false response.
Declarations under Rule 4.17:


- of inventorship (Rule 4.17(iv)) for US only

Published:

- with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
1

AUTHENTICATION OF A SUBSCRIBER STATION

FIELD OF THE INVENTION

The present invention relates to authenticating a subscriber station in a telecommunications system, wherein the identity of the subscriber station is verified on the basis of a subscriber-station-specific secret key stored in the subscriber station. In particular the invention relates to a solution for identifying an authentication message generated by an external attacker.

BACKGROUND OF THE INVENTION

In the GSM system, authentication of a subscriber station is based on a challenge-response procedure. For the authentication, a subscriber-station-specific secret key Ki and an authentication algorithm A3 have been stored in the SIM (Subscriber identity module) card of the subscriber station. The subscriber-station-specific secret key Ki of the subscriber station and the corresponding authentication algorithm A3 have also been stored in an authentication centre of a GSM network. In order to carry out the authentication, a random number generator arranged in the authentication centre first generates a random number and transmits it to a counter as an input. Next, the counter computes a response SRES on the basis of the random number, authentication algorithm A3 and secret key Ki. The authentication centre then transmits the random number and the response SRES to a network element, which carries out the actual authentication, and which, as regards the GSM system, is a VLR (Visitor location register).

The visitor location register forwards the received random number to the subscriber station to be authenticated. The subscriber station comprises a counter, which computes a response SRES based on the received random number, the secret key Ki of the subscriber station and the authentication algorithm A3, and the subscriber station transmits the response SRES to the VLR. The VLR then compares the response transmitted by the authentication centre with the response transmitted by the subscriber station. Since the secret key Ki stored in the memory of the subscriber station is subscriber-station-specific, there is only one subscriber station capable of generating a correct response to the input transmitted thereto. If the responses of the subscriber station and the authentication centre are identical, the subscriber station has been authenticated.
A drawback of the known authentication procedure described above is that it is possible for an external attacker, who desires to crack the secret key stored in the subscriber station, to try to crack the secret key by supplying different inputs to the subscriber station (or the SIM card thereof) again and again and by monitoring the responses being transmitted from the subscriber station. When this procedure is repeated frequently enough and statistics is collected about the inputs and responses, the secret key Ki may be revealed on the basis of the collected data. If the external attacker cracks the key, he or she may be capable of cloning the subscriber station (or the SIM card) by producing a second subscriber station, which has an identical secret key, in which case the cloned subscriber station can be used for making calls, for which the owner of the original subscriber station is billed.

The above problem is solved in PCT/000/00907 such that the system generates authentication inputs comprising MACs (Message authentication code). The subscriber station checks the correctness of the received inputs and maintains a counter function to compute the number of inputs that are incorrect. When a predetermined limit value is exceeded, the subscriber station no longer provides correct responses to the inputs. The problem with this solution is that it requires modifications in the network operator functions, since the system has to be able to generate authentication inputs comprising MACs.

BRIEF DESCRIPTION OF THE INVENTION

An object of the present invention is to alleviate the above-mentioned problem and to provide an improved solution owing to which it is more difficult for an external attacker to crack a secret key of a subscriber station. The objects of the invention are achieved with a method, a system, a subscriber station and a SIM card, characterized by what is stated in the independent claims. The preferred embodiments of the invention are disclosed in the dependent claims.

The underlying idea of the invention is that when an authentication input is received in a subscriber station, the randomness thereof is evaluated. According to the invention, the evaluation of the randomness of a received input is performed utilizing information of one or more inputs received earlier by the subscriber station. If, based on the evaluation, the received input cannot be considered as a random input, it may be a sign of a try to crack the secret key
of the subscriber station. The subscriber station is thus able to identify inputs, which may originate from an external attacker.

The advantage of the invention is that it can with slight changes be applied to existing systems. In the GSM system, for example, the invention can be directly implemented in the SIM card, which means that mobile stations can right from the start be provided with SIM cards capable of checking the randomness of the inputs according to the invention. It is not necessary to change the operation of the network elements, and no changes are required on the subscriber station/network interfaces either.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the invention will be described in closer detail with reference to the accompanying drawings, in which

Figure 1 is a simplified block diagram illustrating the system of the invention,

Figure 2 illustrates the signaling of the invention,

Figure 3 is a simplified flow diagram illustrating the method of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is applicable to any communication system utilizing a random number as a challenge. In the following, embodiments of the invention will be described as implemented in the GSM system without limiting the invention to that particular system.

Figure 1 shows a simplified block diagram of the system S of the invention, showing only the components that are essential to illustrate the invention, even though those skilled in the art naturally know that a general mobile communication system also comprises other functions and structures, which do not have to be described in more detail herein.

Referring to Figure 1, in a mobile system, such as the GSM system, a majority of the authentication equipment of the network N is arranged in a special authentication centre AC, which, in connection with the GSM system, may be located in connection with a home location register (HLR), for example. A GSM system also comprises a mobile services switching centre MSC which enables the communication between the network elements, such as the HLR and the VLR, and the subscriber station MS.
The subscriber station MS (i.e. the mobile station) can be a simplified terminal intended only for speech, or it can be a terminal intended for multiple services operating as a service platform and supporting the loading and execution of different service-related functions. The subscriber station MS comprises the actual mobile equipment and an associated (usually removable) identification card SIM (not shown). The subscriber identity module SIM is a smart card comprising the subscriber identity, executing authentication algorithms and storing authentication and encryption keys and subscriber data needed at the subscriber station. The mobile equipment is a radio terminal used for radio communication between the subscriber station MS and the network N. The mobile equipment can be any equipment or a combination of several different equipment capable of communicating in a communication system.

The blocks shown in the block diagram of Figure 1 may comprise electronic circuits or, alternatively, one or more blocks may be implemented by software. Hence, no two separate counters, for example, are necessary at the subscriber station, but the counters can be implemented, for example, by one processor and computer program in a manner known per se.

In the GSM system, the subscriber station MS is authenticated by a visitor location register VLR such that the VLR receives from the authentication centre AC an input RAND and response SRES enabling the VLR to authenticate the subscriber station MS. The authentication centre AC comprises a first counter for generating a random number RAND. The authentication centre AC also comprises a memory with the secret key Ki stored therein of all those subscriber stations, in the authentication of which the authentication centre participates. In practice, the authentication centre can be operator-specific, in which case all secret keys of the subscriber stations of the operator have been stored in the memory of the authentication centre.

Figure 2 illustrates the successful signaling of the invention when no external attacker is detected. Referring to Figure 2, the authentication centre AC supplies in step 2-1 the secret key Ki of the subscriber station retrieved from the memory and the input RAND produced by the first counter to a second counter. The second counter computes a response SRES on the basis of the secret key Ki, input RAND and authentication algorithm A3. In the message 2-2, the authentication centre AC transmits the input RAND and response SRES to the VLR.
In step 2-3 the VLR stores the response SRES such that it will be available later for a comparing function. In order to authenticate the subscriber station MS, the VLR transmits in the message 2-4 the input RAND received from the authentication centre to the subscriber station MS.

In step 2-5, a comparing unit is activated in the subscriber station MS. According to the invention, the comparing unit evaluates the last received input based on the information of authentication inputs received earlier by the subscriber station. The information of the earlier received authentication inputs comprises samples of earlier inputs that may have been manipulated in an appropriate statistical manner. The comparing unit evaluates if the latest input resembles the information of earlier inputs, and concludes, on the basis of the evaluation, whether the latest input is random or not. The evaluation may be performed utilizing information of randomly selected earlier inputs. An appearance of a non-random authentication input might be a sign of somebody trying to crack the secret key of the subscriber station.

In step 2-5, the MS manipulates the latest input in an appropriate statistical manner with the information of earlier inputs and may store the information such that it is available for later authentications. There may be a predetermined time for how long the information of a received input will be stored. The time for storing the information may also be selected randomly so that the attacker cannot conclude when it would be worthwhile to try to attack again.

If the comparing unit of the MS considers the latest input as a random input, it activates a third counter to compute a response to the input RAND. The third counter computes the response SRES on the basis of the input RAND, the subscriber-station-specific secret key KI stored in a memory of the MS and the authentication algorithm A3. The algorithm is the same algorithm A3 and the parameters are the same parameters as the second counter of the authentication centre AC used. The subscriber station MS produces the response SRES, which is transmitted to the VLR in the message 2-6. The response produced by the MS is supposed to correspond to the response SRES transmitted by the authentication centre AC. If the comparing function of the VLR detects in step 2-7 that the responses are identical, it is concluded that the subscriber station MS has been authenticated.

If, on the other hand, the comparing unit of the MS indicated in step 2-5 that the input RAND is not random, the input has most likely been supplied
by an external attacker, not by an authorized VLR or equivalent. According to
the embodiments of the invention, the subscriber station can be programmed
to operate such that cracking the secret key is made significantly more difficult
when the subscriber station has identified an input originating from an external
attacker.

In one embodiment of the invention, the subscriber station produces
and forwards an input only if the subscriber station has checked the input and
concluded that the input is random. A control unit of the MS interrupts the
process for authenticating the subscriber station such that no response will be
transmitted by the MS. Consequently, it is more difficult to crack the secret key
since an external attacker cannot continue sending inputs and monitoring what
kind of a response each input induces.

In another embodiment of the invention, the subscriber station com-
putes and forwards a false response such as a random response if it detects
that the received input is not random. The random response herein refers to
any response resembling a correct one. The random response may be com-
puted by another algorithm than the authentication algorithm. Alternatively, the
random response may be computed by the authentication algorithm but, in-
stead of the secret key of the subscriber station, the computation utilizes an-
other key, which is a "pseudo key", or, alternatively, the random response may
comprise a random number generated by a random number generator. The
point is that the response is not computed by the authentication algorithm A3,
secret key Ki and input RAND. If this were the case, the external attacker
would be provided with the real response to the supplied input, which might
assist in cracking the secret key. The idea is that the random response resem-
bles a real response such that an external attacker does not, on the basis of
the length of the response, for example, know that the random response is not
a real response provided with an authentication algorithm and a secret key. If,
on the other hand, the external attacker is provided with a random response
resembling the real response, the external attacker will not know that the re-
sponse is an incorrect one.

In yet another embodiment of the invention, the subscriber station
maintains a counter function to compute the number of inputs that are non-
random. In such a case, when a predetermined limit value is exceeded, the
subscriber station locks itself such that it no longer provides a correct response
to the input. In this embodiment, the subscriber station can thus produce and
forward a response, which is either correct or incorrect regardless of whether
the input is random until the counter function indicates that the maximum num-
ber of non-random inputs is exceeded, whereby the authentication function of
the subscriber station is locked. The locking may take place either such that
the subscriber station no longer provides any responses or, alternatively, in
order to mislead the attacker, the subscriber station may continue by producing
incorrect responses only, such as random responses.

Figure 3 is a flow diagram illustrating the method of the invention
when an external attacker is detected. In step 3-1, an authentication message
comprising a non-random input RAND is received in the MS.

According to the first embodiment of the invention, if it is detected
that the input is not random, the processing of the authentication message is
interrupted in step 3-2. No response will then be transmitted to the authentica-
tion message. A notification of interrupting the process may be forwarded in
step 3-3, but this is not mandated by the invention. Consequently, the external
attacker receives no response to the input, which means that the attacker is
unable to collect responses and use them for cracking the secret key.

According to the second embodiment of the invention, if it is de-
tected that the input is not random, a random response is produced to the input
in step 3-4 and forwarded to the sender of the input in step 3-5. The random
response can be any response which resembles a real response and which
has not been computed in a similar manner as the real response. Conse-
quently, the random response can be directly produced by a random number
generator, or it can be computed from the input by utilizing a suitable algorithm
and input. The external attacker will thus receive an incorrect response, how-
ever without knowing this.

According to the third embodiment of the invention, a predetermined
variable Cmax indicating the highest allowed number of non-random inputs
has been stored in the subscriber station (or the SIM card thereof). In addition,
a variable C to keep a record of received non-random inputs is set to a prede-
termined initial value. In this embodiment it is checked in step 3-2 whether or
not variable C utilized by a fourth counter function has reached the limit value
Cmax. If so, this means that the highest allowed number of received non-
random inputs Cmax has already been reached, which means that the authent-
tication process is interrupted as described above in steps 3-2 and 3-3 or a
false response is created as described above in steps 3-4 and 3-5. Otherwise,
the process proceeds according to steps 2-5, 2-6 and 2-7 of Figure 2. When
the counter function of the subscriber station reaches a predetermined limit
value, the authentication functions thereof will be locked such that the sub-
scriber station no longer provides correct responses. When the subscriber sta-
tion is one of the kind, in which the authentication functions are arranged on
the SIM card, such as a GSM mobile station, the subscriber station must next
be provided with a new SIM card to replace the locked one.

The various embodiments of the invention may be carried out simultane-
ously or they may be mutually exclusive. The signalling messages and
steps shown in Figures 2 and 3 are not in an absolute chronological order, and
they can be executed in a different order from the given one. Other signalling
messages can be transmitted and/or other functions can be carried out be-
tween the messages and/or steps. The signalling messages are only examples
and can include only some of the aforementioned information. The messages
can also include other information.

It is possible that necessary parts for checking the inputs and/or pro-
ducing a response in connection with authentication are arranged in the SIM
card or in the subscriber station or both. The invention is also applicable to a
system comprising no SIM cards at all.

It is to be understood that the above description and the related
drawings are only intended to illustrate the present invention. It is obvious to
one skilled in the art that the invention can be modified in various ways without
deviating from the scope and spirit of the invention disclosed in the attached
claims.
CLAIMS

1. A method for identifying authentication messages generated by external attackers, the method comprising receiving authentication inputs in a subscriber station (MS), the method being characterized by evaluating the randomness of a received authentication input utilizing information of earlier-received authentication inputs; and responding in a usual manner to the received authentication input if it is found random.

2. A method as claimed in claim 1, characterized by evaluating the randomness of a received authentication input utilizing information of randomly selected earlier-received authentication inputs.

3. A method as claimed in claim 1 or 2, characterized by locking the authentication process if the received authentication input is found non-random.

4. A method as claimed in claim 1, 2 or 3, characterized by sending a false response to the received authentication input if it is found non-random.

5. A method as claimed in any of the previous claims 1 - 4, characterized by storing information of at least some of the received authentication inputs.

6. A telecommunications system comprising at least one subscriber station (MS) arranged to receive authentication inputs, characterized in that the system is configured to evaluate the randomness of a received authentication input utilizing information of earlier-received authentication inputs; and respond in a usual manner to the received authentication input if it is found random.

7. A subscriber station being arranged to receive authentication inputs, characterized in that the subscriber station is arranged to evaluate the randomness of a received authentication input utilizing information of earlier-received authentication inputs; and respond in a usual manner to the received authentication input if it is found random.

8. A SIM card being arranged to receive authentication inputs, characterized in that the SIM card is arranged to
10

evaluate the randomness of a received authentication input utilizing information of earlier-received authentication inputs; and

respond in a usual manner to the received authentication input if it is found random.

9. A SIM card as claimed in claim 8, characterized in that it is arranged to evaluate the randomness of a received authentication input utilizing information of randomly selected earlier-received authentication inputs.

10. A SIM card as claimed in claim 8 or 9, characterized in that it is arranged to lock the authentication process if the received authentication input is found non-random.

11. A SIM card as claimed in claim 8, 9 or 10, characterized in that it is arranged to send a false response to the received authentication input if it is found non-random.

12. A SIM card as claimed in any of the previous claims 8 - 11, characterized in that it is arranged to store information of at least some of the received authentication inputs.
Fig. 2
Fig. 3

Receive non-random input in MS

3-1

3-2
Interrupt the authentication

3-3
Send a notification of interruption

3-4
Calculate an incorrect response

3-5
Forward the incorrect response

Fig. 3
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNIAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>WO 0213568 A1 (ORANGE PERSONAL COMMUNICATIONS SERVICES LIMITED), 14 February 2002 (14.02.02), page 4, line 21 - page 15, line 13</td>
<td>1-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>US 2002180583 A1 (LAURI PAATERO ET AL), 5 December 2002 (05.12.02), abstract</td>
<td>1-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>WO 0189253 A1 (ICO SERVICES LTD.), 22 November 2001 (22.11.01), abstract</td>
<td>1-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>US 2003003895 A1 (PONTUS WALLENTIN ET AL), 2 January 2003 (02.01.03), abstract</td>
<td>1-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
  “A” document defining the general state of the art which is not considered to be of particular relevance
  “E” earlier application or patent but published on or after the international filing date
  “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  “O” document referring to an oral disclosure, use, exhibition or other means
  “P” document published prior to the international filing date but later than the priority date claimed
  “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
  “X” document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
  “Y” document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
  “&” document member of the same patent family

Date of the actual completion of the international search

2 December 2003

Date of mailing of the international search report

4 12 2003

Name and mailing address of the ISA/
Swedish Patent Office
Box 5055, S-102 42 STOCKHOLM
Facsimile No. + 46 8 666 02 86

Authorized officer

Stefan Hansson/mj
Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>WO 0213568 A1</td>
<td>14/02/02</td>
<td>AU 7647601 A</td>
<td>18/02/02</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1444835 T</td>
<td>24/09/03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1305969 A</td>
<td>02/05/03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 0019110 D</td>
<td>00/00/00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 2366938 A</td>
<td>20/03/02</td>
</tr>
<tr>
<td>US 2002180583 A1</td>
<td>05/12/02</td>
<td>AU 7928000 A</td>
<td>30/04/01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1382357 T</td>
<td>27/11/02</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1224827 A</td>
<td>24/07/02</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FI 992258 A</td>
<td>20/04/01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FI 992595 A</td>
<td>19/04/01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2003512792 T</td>
<td>02/04/03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0130104 A</td>
<td>26/04/01</td>
</tr>
<tr>
<td>WO 0189253 A1</td>
<td>22/11/01</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>US 2003003895 A1</td>
<td>02/01/03</td>
<td>WO 02093970 A</td>
<td>21/11/02</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002168984 A</td>
<td>14/11/02</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 02093971 A</td>
<td>21/11/02</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2003050097 A</td>
<td>13/03/03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 03043364 A</td>
<td>22/05/03</td>
</tr>
</tbody>
</table>

Form PCT/ISA/210 (patent family annex) (July 1998)