SUBMISSION NO. 61

Dr. Peiyuan Zhu

27 August 2009

Jane Hearn
Inquiry Secretary
Committee Secretary
Standing Committee on Communications
House of Representatives
Parliament House
CANBERRA ACT 2600
AUSTRALIA

Re: Terms of Reference f) Emerging technologies to combat these risks.

Dear Jane Hearn

Thank you for your email dated 26 August 2009.

I would like to bring your committee awareness of an invention I made that can be a very effective method to combat cyber crime.

My invention provides a new method that can be easily adopted in almost any applications where transferring critical electronic data through the net are necessary. It should be particularly suitable for high-end users/applications where higher security level cyber protection is desirable.

Using my method, the critical data is to be masked in a unique way for each user and for each occasion. The fact that the unique masking method is randomly selected on spot and valid once only makes hijacking the masked critical data pointless.

A typical example of the critical data that obviously need protection is “login password”. However, this invented method can find far more applications than just protect password from hijacking.

For detailed description of my invention I refer to the full specification of my invention which is attached here as well.

You are welcome to contact me if you have any interest in knowing more about this technology and its potential applications.

Yours truly,

Dr. Peiyuan Zhu

(12) STANDARD PATENT APPLICATION (11) Application No. **AU 2006201037 A1**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Masked identification system

(51) International Patent Classification(s)
H04L 9/00 (2006.01)

(21) Application No: **2006201037** (22) Date of Filing: **2006.03.09**

(30) Priority Data

(31)	Number	(32)	Date	(33)	Country
	2005901301		**2005.03.17**		**AU**

(43) Publication Date: **2006.10.05**
(43) Publication Journal Date: **2006.10.05**

(71) Applicant(s)
Peiyuan Zhu

(72) Inventor(s)
Zhu, Peiyuan

(74) Agent / Attorney
Peiyuan Zhu,

ABSTRACT

The disclosed Masked Identification System is a new method that provides the user a more secure environment for passing and identifying critical data through public and/or private computer related facilities. The system uses an Implied Masking System and a Decoding System to eliminate the needs of passing critical data directly from a remote user-end to the central system. For each occasion, the Implied Masking System generates an instance implied masking instruction, which implies a unique masking method that is meaningful only to a genuine user, through the default user rules provided to the user. The critical data can then be masked into a format that only the central system should be able to understand. The decoding section of the Masked Identification System converts or checks the validation of the masked data received and accepts only those masked with the implied method for the occasion. The system thus provides protection for remotely accessing, identifying or passing critical data since the data going through any network is masked in a secure way and therefore meaningless to any third party should it be hijacked. This invention can be used in any electronic logon process or any other process that requires identifying registered critical data for eliminating all threats from internet thefts.

2006201037 09 Mar 2006

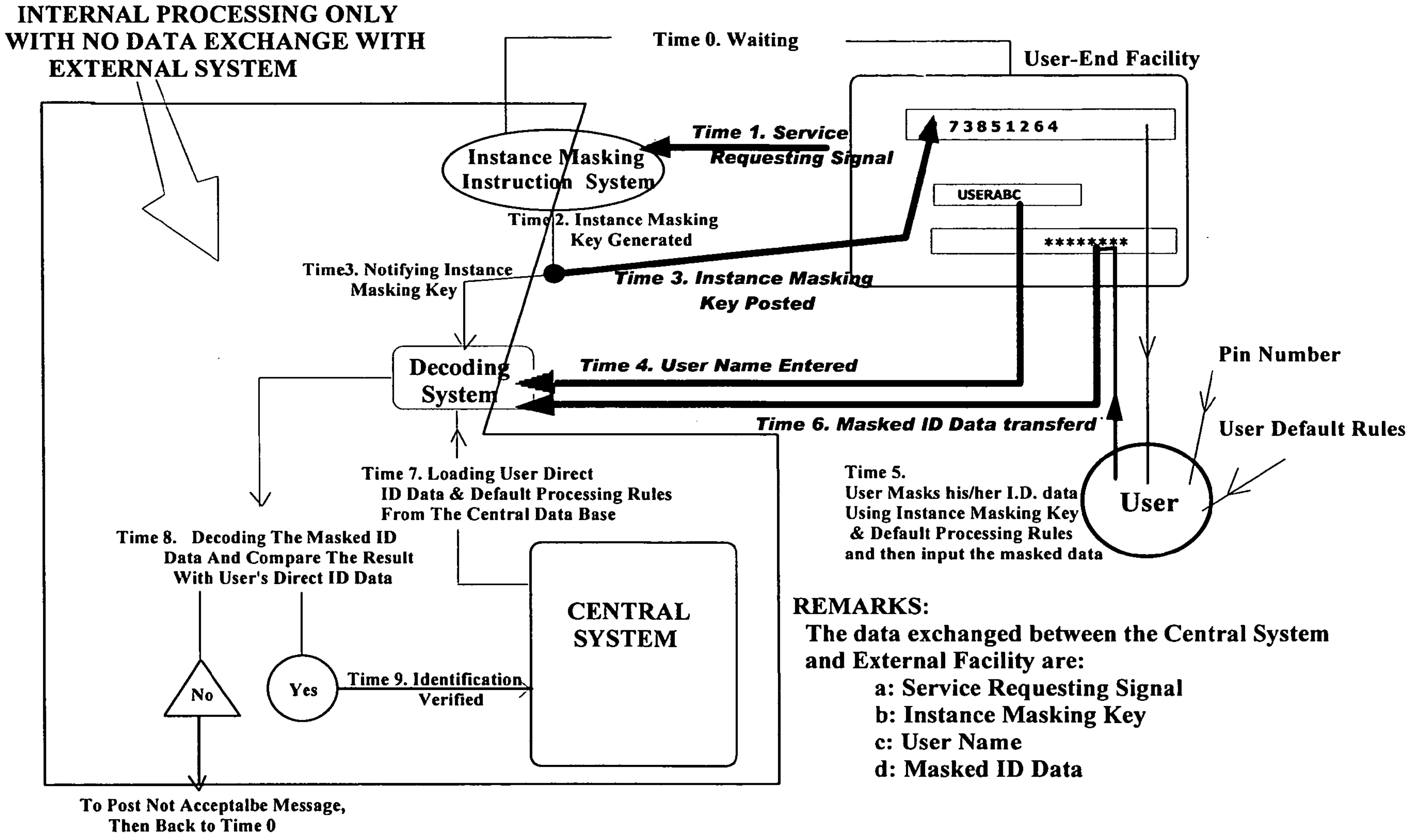
AUSTRALIA

Patents Act 1990

COMPLETE SPECIFICATION
STANDARD PATENT

MASKED IDENTIFICATION SYSTEM

The invention is described in the following statement:


INTERNAL PROCESSING ONLY
WITH NO DATA EXCHANGE WITH
EXTERNAL SYSTEM
Time 0. Waiting
User-End Facility
Time 1. Service Requesting Signal
Instance Masking Instruction System
73851264
USERABC
****
Time 2. Instance Masking Key Generated
Time3. Notifying Instance Masking Key
Time 3. Instance Masking Key Posted
Decoding System
Time 4. User Name Entered
Pin Number
User Default Rules
Time 6. Masked ID Data transferd
Time 7. Loading User Direct ID Data & Default Processing Rules From The Central Data Base
Time 5. User Masks his/her I.D. data Using Instance Masking Key & Default Processing Rules and then input the masked data
User
Time 8. Decoding The Masked ID Data And Compare The Result With User's Direct ID Data
CENTRAL SYSTEM
No
Yes
Time 9. Identification Verified
To Post Not Acceptalbe Message, Then Back to Time 0

REMARKS:
The data exchanged between the Central System and External Facility are:
a: Service Requesting Signal
b: Instance Masking Key
c: User Name
d: Masked ID Data

Figure 1. Event Flow Chart For One Format Of A Simple Masked Identification System

MASKED IDENTIFICATION SYSTEM

This invention relates to improvements in providing a secure environment for critical data identification process through public and/or private computer related facilities.

Security is an important issue in any process involving passing critical data in computer related facilities. Many service providers have now provided their clients options for using their services remotely through computer related facilities, often relying on a public network for data exchange. The fear of critical data (especially those for user/client identity) being stolen or hijacked during the data transfer process has limited the usage of these options. It is a real threat to many users that credit card numbers or other identity related data might be stolen as they are passing through a public network system.

Most current available security methods in relation to protecting identity related information are aimed to prevent the information being stolen or leaked during the data transfer process. These security systems are based largely on the assumption of a third party's inability of accessing these data in the network since the security protection methods would make it difficult for a third party doing so.

This invention proposes a totally different approach, which does not try to prevent possible leakage of the data during the transfer process, but rather makes the transferred data meaningless for any third party. Therefore, the system provides security protection even when all the data transferred in the network are hijacked.

The Masked Identification System contains an Implied Masking System and a Decoding System, named according to their main functions.

The Implied Masking System works in such way that the central system provides a masking method in an implied manner for each occasion and the user masks the critical data according to the method. Only the masked data is to be transferred to central system, which does not need to contain any meaningful information to a third party. The threat from critical data being stolen during the process is thus eliminated, since the critical data never appear in the system.

The Decoding System is responsible to check the validation of the masked data.

The Implied Masking System realizes its function through two main components: an Instance Masking Instruction System and a Default User Rule System.

The Instance Masking Instruction System generates a masking instruction (an instance implied masking instruction, or IIMI for short, through out this invention) for each occasion. The generation of the IIMI can be through a random selection process or any other method. Once an IIMI is generated, it will be posted to the user-end facility.

An instance implied masking instruction (IIMI) can be in any format. For example, it can contain colours, shapes, alphabets, numbers or any other elements as far as it can imply certain information. It can be very detailed with full description and explanation for each term it used, or be very brief by assuming the meaning of certain terms in the instruction as common knowledge.

One format of the IIMI, for example, can be a matrix of digits to indicate a necessary masking method. The random generation of such masking instruction can be easily obtained through a rather simple piece of computer program.

An IIMI alone does not contain any masking method. It is an instruction from the central system to all the users, and it alone does not define any anything. Therefore, leaking of an IIMI in the internet would not pose any security threat.

By introducing private default user rules, this invention makes it possible for a posted IIMI to imply different masking methods for individual users without needing to know who is to use it.

The Default User Rule System is to allow a user to get the relevant information from an IIMI. The information can then be used to determine a current masking method for the user.

Since IIMI vary for each occasion, the masking method is then different for each occasion.

A masking method is thus only defined at the time of a user's accepting an IIMI, and it is defined jointly with the posted IIMI and the user's private default user rules.

Similar to any other critical data, such as pin number or password, private default user rules are given to the user alone, and are to be managed in the central system for maximising user protection.

In general, each user/client will be given unique private default rules.

This invention thus extends the region of critical identification information to include the default user rules, which can be in various formats. The critical identification information will remain the secrets between the genuine user and the service provider. The Masked Identification System eliminates the needs for passing them directly in any data transfer process for the purpose of identification.

The following two simple examples, based on a given received IIMI that is a simple six digits number series (+1, -0, -2, +9, -4, -2), demonstrate the application of default user rules to get relevant information from IIMI. The relevant information can then be used to obtain a masking method.

- Default Rule -- Read backward.

The relevant information the user will obtain from the IIMI is then:
-2, -4, +9, -2, -0, +1.

- Default Rule – Using opposite sign.

In this case, the relevant information the user will get from the IIMI is:
-1, +0, +2, -9, +4, +2.
The examples are only to demonstrate that even a very simple given IIMI provides differently information for users with different default user rules.

An IIMI can contain far more information than necessary.

It would be practical that the definition of certain common terms as part of user rules, or part of IIMI, be given to the user community. These terms can then be used without explanation for simplicity.

This invention does not limit the number and the complexity of either the instance implied masking instruction and/or the default user rules. The complexity of the entire implied masking system can be adjusted to suit the needs for various applications. It can be simple enough that no Default User Rule is involved at all, or be very complicated using sophisticated procedures, depending on whatever a relevant service provider believes to be necessary.

Overall, the Instance Masking Instruction System makes sure the IIMI for each occasion will be different, while the Default User Rule System guarantees that only the genuine user will understand the implied masking method for him/her from the posted instance implied masking instruction.

With the implied masking method, the critical data can be masked outside any network connected facility. Therefore no information can be stolen or hijacked during the masking process.

It should be noticed that the Instance Masking Instruction System and the Default User Rule System are only names to refer the main functions of certain part of system this invention is specifying. They can be physically linked together or mixed together. An element of these systems does not have to be any physical component. It can even be a manual operated process. For example, a process of user's selectively reading a posted IIMI, according to certain private default user rules, serves the function of identifying relevant information from IIMI, therefore the process is an element of the Default User Rule System.

The Masked Identification System will only accept the data masked using the specified implied masking method for a genuine user, which is valid only for one occasion and is meaningless for a third party even if they are stolen or hijacked.

Since the critical data and private default user rules would never need to be transferred in the computer or network system, therefore it is not possible for them to be stolen there.

A masking process can be designed as an irrevocable process, so that the masked dada would have no correlation with the password, user rules and the information contains masking instruction. Since only the masked data will be used to identify a genuine user's critical data, this technology can make it possible even in theory to eliminate all the threats from internet hijacking in terms of critical data protection.

The Decoding System in the central machine is responsible for checking the validation of the masked critical data. Upon the receiving of an activation signal, the Decoding System loads the relevant critical data and the relevant default user rules from a central database. The decoding is a reverse processing of masking or simply a generation of the same masked critical data for comparison purpose. With all the necessary information available in the central system, it is a simple matter to implement a Decoding System.

Since the decoding system is located in the central system and no data transfer to any external systems is to be involved, therefore, there is no decoding data to be stolen or hijacked in the network.

As specified above, the method of a Masked Identification System can be summarised as following:

- In addition to the critical data for user identification, individual user is also provided with certain private default user rules.
- The system generates IIMI and posted in the user-end computer or other facilities.
- By combining private user rules and the relevant information from the posted IIMI, the user gets the implied masking method for an identification instance and then masks the critical data using the method outside any facility that is connected to any network.
- The user only inputs the masked data to the facility.
- The validation of the masked data will be checked by the decoding system for the purpose of identification.

Using the Masked Identification System, the only identification related data need to be transferred between the user-end computer and the central system would be the IIMI and the masked identification data. These data are not critical any more since the IIMI alone does not contain masking method, while the masked identification data will be valid only in the current identification occasion. In general, a properly designed masking method can make sure the masked data have correlation with the relevant critical data, IIMI and the user rules that they are comes from, especially in the case of using a irrevocable masking method. Therefore, it is generally safe even both masked data and posted IIMI are leaked into other hands, since they are of no use for others.

Although the present invention provides a new method that works even in the case of all the data exchanged between the user-end and the central system being monitored, hijacked, or stolen by a third party, the method itself does not imply such hijacking should be invited. The present invention can be added to most currently available security methods to provide double security assurance for the purpose of lifting client's confidence for using remote computer related facilities.

To assist with understanding of the concept of this invention, reference will now be made to the accompanying figures.

Figure 1 is an event flow chart of an example of a Masked Identification System as one format of this invention, with remarks about the type of data being exchanged between the internal and external systems during the process. In figure 1, IIMI is presented as an 8 digits instance masking key for simplicity.

Figure 2 shows an example of the user interfaces in a computer related facility, showing an IIMI in the format of an instance masking key containing 6 digits. It also includes an example of the masking process with no private Default User Rule as a special extreme case. A common user rule of simply plus is used in this case.

Figure 3 shows an example of the user interfaces in a computer related facility, showing an IIMI. It also includes an example of the masking process using an implied masking method with two default user rules.

In figure 2 and figure 3, a definition of a simple single digit processing rule is assumed as an additional common default rule such that if the normal result of A+B is over 10 then minus the result by 10; if A is less than B, then A - B to be treated as A+10–B, where A and B are both single digit positive numbers.

Figure 4 shows an example of irrevocable masking using the method implied by an IIMI and private user rules.

Figure 5 shows a function chart of an electronic logon system as an example of one format of the application of this invention, with remarks about the roles the user, the user-end computer, and the service provider's central system are taking respectively.

Referring to Figure 1 it can be seen that the sample security system works in the following time frames: an Instance Masking Instruction System generates an instance implied masking instruction when the system is signaled, posts it to the user-end facility and informs the Decoding System. The user enters user name and converts the posted instruction into the implied masking method using his/her default user rules. Upon the receiving of USERNAME, the Decoding System loads the relevant information from the central database and prepares for checking the masked data for this occasion from this user. After a masking process, the user inputs his/her masked I.D. data, which signals the Decoding System for a decoding process. The outcome of the decoding process will result in an approval or a rejection of the identification.

Referring to Figure 2 it can be seen that the masking process can be rather simple, and the process can be done without any tool for most people, but including certain default user rules can significantly increase the protection level of this sample.

Referring to Figure 3 it can be seen that the Implied Masking System works much better with the involvement of just two simple default user rules, with comparison to the sample showing in Figure 2. The masked pin number is meaningless to a third party who has no knowledge of the default rules.

Referring to Figure 4 it can be seen that an irrevocable masking process can be rather easily designed. It also shows an example that the IIMI contain much more data than to be used for one single user. A particular way to obtain relevant information from the IIMI, in this example, a user's activity of selectively reading the IIMI according to the unique positions given to the user, is here a valid part of the private default user rules. Obviously, the usage of the private default user rules in such an activity will not be subject to any threat from any internet hijacking. Although a common electronic calculator would be handy here, the actual masking step in this example is not depending on any device. This example shows that by designing an irrevocable masking process, it is possible to process the identification with masked data that comes from the critical data but does not really contain any information about or with any correlation with the critical data any more.

Also referring to Figure 4, it can be noticed that all through the relevant locations of the IIMI for a user in this sample is described as five pairs of coordinates, these locations can be memorised by the user as a V shape starts at the second element of the first line. A particular shape is normally easier for most people than to memorise an additional password. Therefore introducing private default user rules as additional critical identification data can be rather feasible if the rules are designed and chosen properly.

Referring to Figure 5 it can be see that this invention can be readily used as an electronic logon system. By designing the structure of IIMI and the masking method similar to that described in Figure 4, such an electronic logon system can eliminate all threats from any internet hijacking activities, since the critical data, the user password and the private default user rules, will only be used in the steps outside the computer system

It should be noticed that the examples in Figures 1-5 only serve the purpose for a better understanding of this invention, and the format of this invention is not limited by them in anyway. In fact, there are an unlimited number of possible implied masking methods and an unlimited number of possible IIMI formats this invention can use.

The invention does not limit the method of masking and the format of IIMI, which can be designed to suit the needs of any particular application. The masking method can be designed to be so simple that the masking process can be worked out just in one's mind for most users. The method can also be designed in a way that certain electronic device, specially designed or commonly available (such as a calculator), can be used as a convenient tool for an easier masking. The device involved for this purpose alone does not need to contain any secret or be registered, since the masking process is not really relying on it.

This invention provides a safe method of critical data identification without actually passing the data. The method uses a principle of never passing anything that could be used by a third party in the system, therefore provides security protection for the identification process. The identification is realized through checking the validation of masked data which is masked according to an implied masking method. The implied masking method is defined through a posted Instance implied masking instruction and certain private default user rules which only a genuine user has access to.

The claims defining the invention are as follows:

1. A masked identification system comprising a method of registered critical data identification through a data masking process, which using a masking method that is implied to a user for an individual occasion, and a validation check process of the masked data in the central system.

2. The masked identification system of claim 1 wherein the method of registered critical data identification does requires inputting the registered critical data into any facility that might be at risk due to any possible internet hijacking.

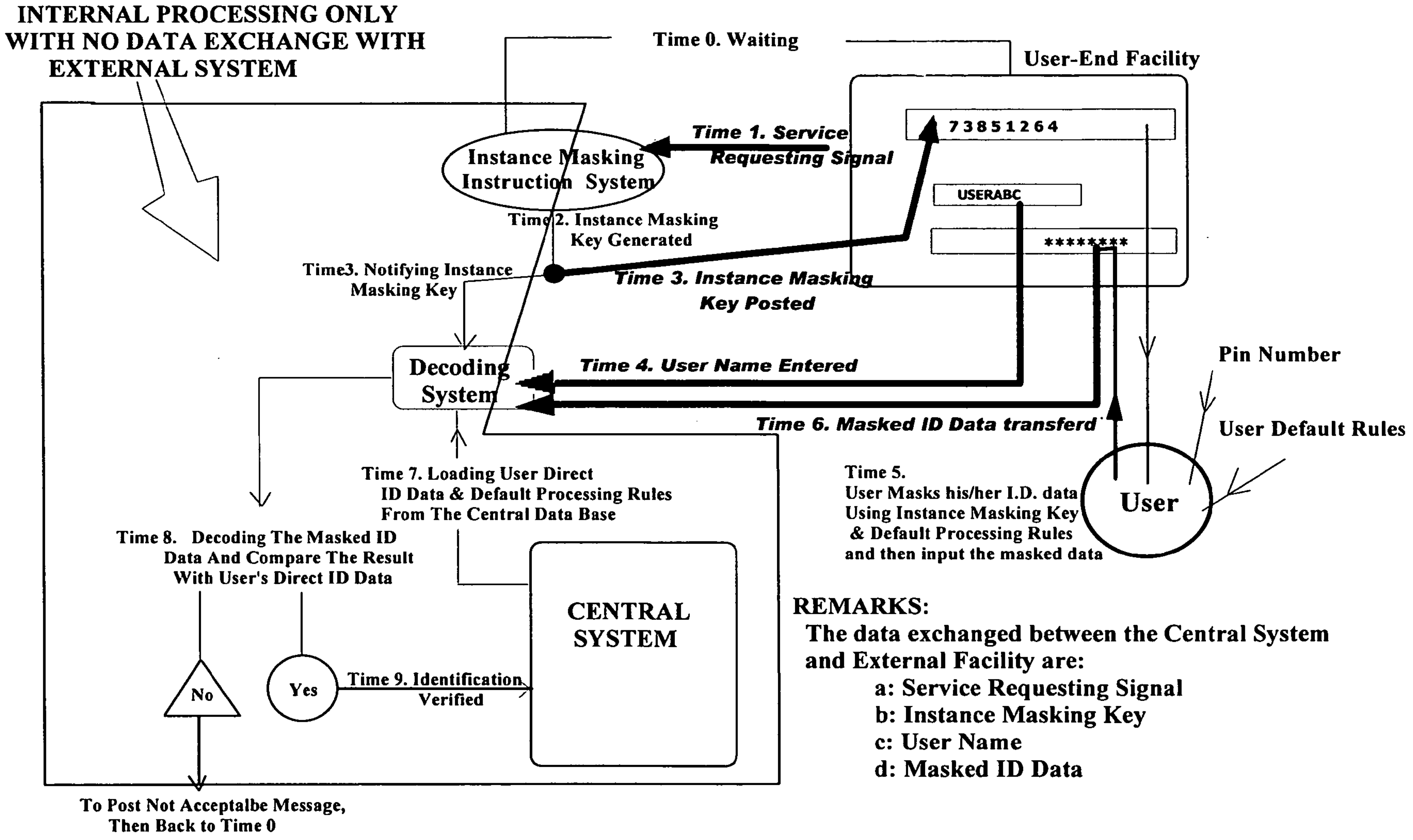
3. The masked identification system of claim 1 wherein the data masking process comprising data masking with a method that is implied to the user through an instance implied masking instruction generated for each identification occasion that is meaningless but to a genuine user.

4. The masked identification system of claim 1 to 3 wherein the data masking process comprising the usage of private default user rules that are provided only to a registered user for the purpose of defining masking methods relevant only to the user from instance implied masking instructions.

5. The masked identification system of claim 1 to 4 wherein the data masking process comprising a step of using the registered critical data for the purpose of masking without needing to involve any device or computer that is linked or registered with any other system in any way.

6. A masked identification system as hereinbefore described substantially with reference to the accompanying figure 1 to 5.

DATED THIS 8TH DAY OF MARCH 2006
PEIYUAN ZHU

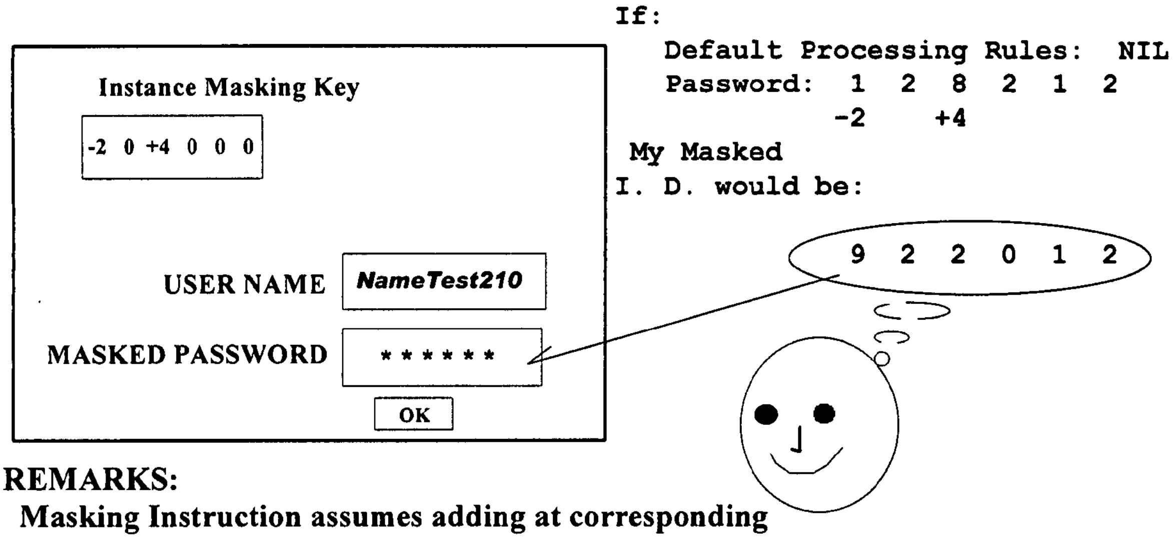

INTERNAL PROCESSING ONLY
WITH NO DATA EXCHANGE WITH
EXTERNAL SYSTEM
Time 0. Waiting
User-End Facility
73851264
USERABC
****
Time 1. Service Requesting Signal
Instance Masking Instruction System
Time 2. Instance Masking Key Generated
Time3. Notifying Instance Masking Key
Time 3. Instance Masking Key Posted
Decoding System
Time 4. User Name Entered
Pin Number
User Default Rules
Time 6. Masked ID Data transferd
User
Time 5.
User Masks his/her I.D. data
Using Instance Masking Key
& Default Processing Rules
and then input the masked data
Time 7. Loading User Direct ID Data & Default Processing Rules From The Central Data Base
Time 8. Decoding The Masked ID Data And Compare The Result With User's Direct ID Data
CENTRAL SYSTEM
No
Yes
Time 9. Identification Verified
To Post Not Acceptalbe Message, Then Back to Time 0

REMARKS:

The data exchanged between the Central System and External Facility are:

a: Service Requesting Signal
b: Instance Masking Key
c: User Name
d: Masked ID Data

Figure 1. Event Flow Chart For One Format Of A Simple Masked Identification System



Instance Masking Key

-2 0 +4 0 0 0

USER NAME NameTest210

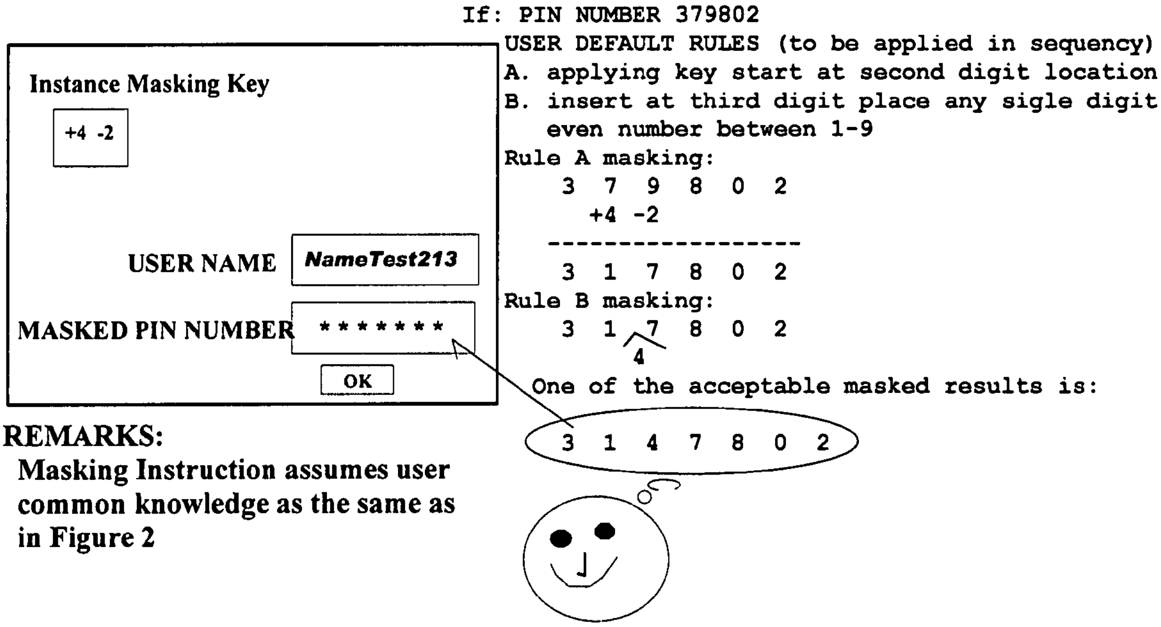
MASKED PASSWORD * * * * * *

```
If:
   Default Processing Rules:  NIL
   Password:  1  2  8  2  1  2
                 -2    +4
 My Masked
I. D. would be:
              9  2  2  0  1  2
```

REMARKS:

Masking Instruction assumes adding at corresponding location and take only the last digit should any adding results in two digits number as user common knowledge also assume a-b be converted as a+10-b should a < b as common knowledge

Figure 2. An Example Of User-End Window And A Simple Masking Process



Instance Masking Key

+4 -2

USER NAME NameTest213

MASKED PIN NUMBER * * * * * * *

```
If: PIN NUMBER 379802
USER DEFAULT RULES (to be applied in sequency):
A. applying key start at second digit location
B. insert at third digit place any sigle digit
   even number between 1-9
Rule A masking:
    3  7  9  8  0  2
       +4 -2
   -----------------
    3  1  7  8  0  2
Rule B masking:
    3  1 ^7  8  0  2
         4
 One of the acceptable masked results is:
    3  1  4  7  8  0  2
```

REMARKS:

Masking Instruction assumes user common knowledge as the same as in Figure 2

Figure 3. An Example Of User-End Window And An Implied Masking Process Involving Two User Default Rules

- **Posted IIMI:**

3	5	6	8	1	4	2	7	9	5
2	1	5	6	7	3	8	0	4	9
6	9	3	1	5	8	7	3	0	2
4	3	1	6	2	5	0	9	8	7
1	9	2	0	6	3	4	8	3	7
0	7	8	6	4	5	7	1	2	9
4	4	7	3	9	1	8	4	5	0
9	2	3	1	6	7	0	5	8	4
5	3	4	1	8	2	5	9	1	3
8	6	0	9	1	6	3	2	6	8

- Password : 36857
- User Rule rules:
  - Get the relevant elements, by just looking at the "user" locations of (1,2); (2,3); (3,4); (2,5); (1,6) in the IIMI. Uses these element to form a factor. In this case, it is 55174.
  - Times the password by the factor and take part of the result (for this example, delete first and fifth digits and take the first 6 digits, this can be designed as a common user rule) as masked password.

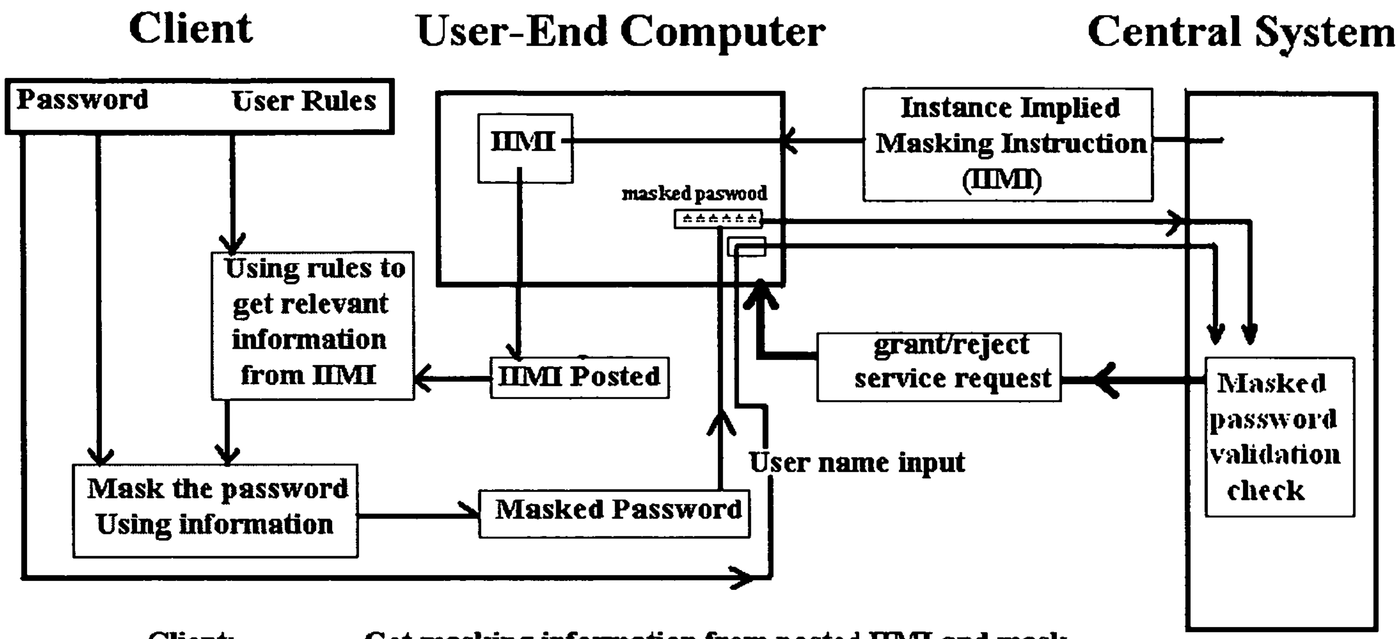
36857 x 55174 = 2033548118

Masked password: 033481

Since only part of the multiplication result is taken as masked password, the masking is an irrevocable process and one can not trace the password or other information back from the masked password.

Notice the posted IIMI will be different for each occasions, the masked password worked out for this occasion will have no value for any other occasions.

Figure 4: An example of irrevocable masking using the method implied by an IIMI and private user rules


Client
User-End Computer
Central System
Password
User Rules
IIMI
masked paswood
Instance Implied Masking Instruction (IIMI)
Using rules to get relevant information from IIMI
IIMI Posted
grant/reject service request
Masked password validation check
User name input
Mask the password Using information
Masked Password

Client: Get masking information from posted IIMI and mask
the password accordly. Input masked password and user name.

User computer: Receive and post IIMI on screen, take masked password
and forward it to the central system

Central System: Generate IIMI and send it to user computer. Receive user name &
masked password and check its validation. Grant or
reject service request accordingly

Figure 5: Function block Chart of an application of the Masked Identification System as an electronic Logon system. Here the registered critical data to be identified is the password. Notice the blocks in shade are the steps outside the computer hence not subject to any internet hijacking threat