



- (51) International Patent Classification:
H04L 9/32 (2006.01) *G06F 21/44* (2013.01)
- (21) International Application Number:
PCT/MY2015/050028
- (22) International Filing Date:
6 May 2015 (06.05.2015)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
PI2014701263 16 May 2014 (16.05.2014) MY
- (71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, Kuala Lumpur, 57000 (MY).
- (72) Inventors: **LOW, Swee Leong @ Low, Kwang Hao**; c/o Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **OOI, Hoey Yew**; c/o Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **KHALID, Putri Shahnim**; c/o Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY).
- (74) Agent: **CHUAH, Jern Ern**; Advanz Fidelis Sdn Bhd, Suite 609, Block D, Phileo Damansara 1, No 9 Jalan 16/11, Petaling Jaya, Selangor, 46350 (MY).

- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- as to the identity of the inventor (Rule 4.17(i))
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR ACCESSING A NETWORK

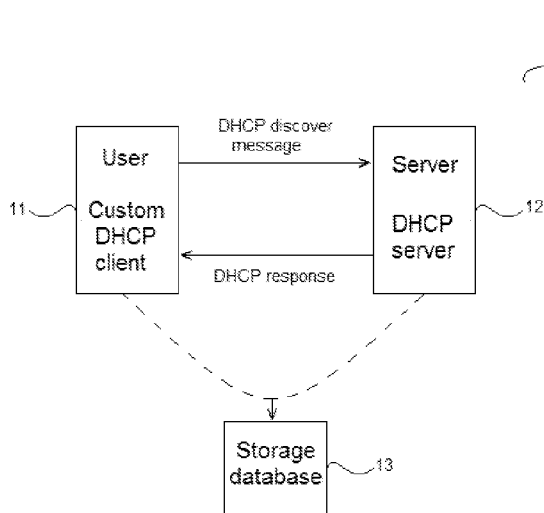


Figure 1

(57) Abstract: The present invention discloses a system (1) and method (2) for accessing a network that is capable of controlling and securing user access into the network. The system (1) and method (2) discloses that the user (11) provides secured information to the server (12) in a message in order for the server (12) to identify and decrypt the secured information based on the access information and thereafter provides access into the network to the user (11) when the secured information is decrypted.



— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SYSTEM AND METHOD FOR ACCESSING A NETWORK

TECHNICAL FIELD OF THE INVENTION

The invention relates to network communications and in particular providing a
5 system and method for accessing a network.

BACKGROUND OF THE INVENTION

The Dynamic Host Client Protocol (DHCP) is used to automatically assign network configuration parameters such as Internet Protocol (IP) addresses to
10 devices for connecting to a network. A conventional DHCP system where once a device is plugged into a local network, the Media Access Control (MAC) address of the device is sent over to the network within the DHCP protocol. However, the MAC address sent over the network within DHCP protocol is not a spoof proof method. One can easily change the MAC address and gain access to the local
15 network. This breach of security therefore poses as a threat for high security organizations as any user can sneak into the server with a spoof MAC address and gain access to the network.

The current DHCP systems are not equipped to handle authentication especially
20 when the first message is sent to the server by an uninitialized device. Hence, an unauthorized personnel inside or outside the network can easily abuse the network. Virus creation kits, hostile software, logical bombs and remote access tools are examples of compromises the network security faces and these are seldom detected by computer virus software.

25

In view of the abovementioned security threats, several methods have been developed to provide a secured network access including firewalls which has been an integral part of network protection.

30 US patent application number 20010047484 A1 discloses a system which integrates Kerberos Security with a dynamic address assignment scheme, i.e. DHCP. The method discloses an uninitialized client obtaining credentials from a

server which is then used to provide authenticated exchange for network configuration parameter assignment. However, the method can only be used in systems that integrate Kerberos Security.

- 5 US patent number 7,983,418 B2 discloses a method to provide an improved support of DHCP service for a DHCP client. The method disclosed provides a robust solution for authentication as well as authorization for DHCP services. This method is performed by implementing an Authentication, Authorization and Accounting (AAA) infrastructure to assign the appropriate DHCP server to a
10 DHCP user. This method only identifies the user and without further identification, the DHCP protocol can be susceptible to spoof user identification entering the network.

- A research paper entitled "The Secure DHCP System With User Authentication"
15 addresses the security threat mentioned above by introducing a user authentication and a session between the sending of messages from a DHCP server and DHCP client. This method prevents unauthenticated users from obtaining an IP address from the DHCP server. However no part of the paper discloses the use of a session to authenticate both the user identity and the
20 device identity.

In terms of security protection, the existing methods have their limitations. Therefore, it is an aim of this present invention to provide a system and method that is capable of securing and controlling network access.

25

SUMMARY OF THE PRESENT INVENTION

- The present invention relates to a system and method for accessing a network. The system comprises at least a user that requires access into a network, at least a server that allows the user to access the network based on access information
30 of the server and a secured information provided by the user, at least a storage database for receiving and storing the access information and the secured information, characterized in that the user provides the secured information to the

server in a message in order for the server to identify and decrypt the secured information based on the access information and provides access into the network to the user when the secured information is decrypted.

- 5 The method for accessing a network comprising the steps of sending a message to a server by a user to request access into a network, determining whether there is a secured information in the message provided by the user, obtaining access information from the storage database when the server determines that the secured information is in the message, decrypting the secured information using
10 the access information obtained from the storage database, and providing access into the network to the user when the secured information is decrypted by the server.

- It is an object of the present invention to provide a system and method for
15 accessing a network that is capable of controlling user access into the network.

It is another object of the present invention to provide a system and method for accessing a network that is capable of securing user access into the network.

- 20 It is further an object of the present invention to provide a system and method that decrypts secured information provided by a user based on the access information of the server prior to the provision of access to the user into the network.

- 25 It is still further an object of the present invention to provide a system and method that decrypts secured information comprising user identification and device identification prior to the provision of access to the user into the network.

BRIEF DESCRIPTION OF THE DRAWINGS

- 30 Figure 1 illustrates the system for accessing a network, as described in the present invention.

Figure 2 illustrates the flow diagram of the method for accessing a network, as described in the present invention.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

5 The above mentioned and other features and objects of this invention will become more apparent and better understood by reference to the following detailed description. It should be understood that the detailed description made known below is not intended to be exhaustive or limit the invention to the precise form disclosed as the invention may assume various alternative forms. On the
10 contrary, the detailed description covers all the relevant modifications and alterations made to the present invention, unless the claims expressly state otherwise.

The present invention discloses a system (1) and method (2) for accessing a
15 network. The system (1), as illustrated in Figure 1, comprises at least a user (11) that requires access into a network, at least a server (12) that allows the user (11) to access the network based on access information of the server (12) and a secured information provided by the user (11), at least a storage database (13) for receiving and storing the access information and the secured information,
20 characterized in that the user (11) provides the secured information to the server (12) in a message in order for the server (12) to identify and decrypt the secured information based on the access information and provides access into the network to the user (11) when the secured information is decrypted.

25 One of the embodiment of the present invention discloses that the user (11) is a Dynamic Host Client Protocol (DHCP) client user, which the user (11) may be a device that has a custom DHCP client installed within the device. In order to access the network, the user (11) first sends a message to the server (12). The server (12) mentioned herein is a Dynamic Host Client Protocol (DHCP) server.
30 The message that the user (11) sends to the server (12) is a Dynamic Host Client Protocol (DHCP) message, where it contains secured information. The secured information is a configuration parameter obtained from the user (11) and the

user's device, which the configuration parameter comprise one or a combination of user identification and device identification. The user identification is obtained by prompting the user (11) with the insertion of a key configuration, or in other words, a password. The device identification is one or a combination of serial number or international mobile subscriber identity (IMSI) of the device. The serial number may also be a hard disk serial number.

Thereafter, the custom DHCP client in the user's (11) device calculates a value by encrypting the device identification with a key generated by a hash message algorithm of the user identification. The value is a 64 bytes message embedded within a DHCP vendor extension message field with a code of 231, which forms the secured information.

Upon receiving the DHCP message from the user (11), the server (12) first determines whether the message contains the secured information. If so, the server (12) extracts Media Access Control (MAC) address of the device and uses the address as a key to locate the access information. The access information is used as a decryption key to decrypt the secured information provided by the user (11). Upon decrypting the secured information, the server (12) parses the decrypted secured information and conducts a check in the storage database (13) to determine whether the decrypted secured information matches the access information. If so, the server (12) will respond to the user (11) by providing access into the network to the user (11).

The method (2), as illustrated in Figure 2, for accessing a network comprises a first step to send a message to the server (12) by the user (11) (- 21) to request access into a network. Prior to the sending of the message, the custom DHCP client in the user's device calculates a value by encrypting the device identification with a key generated by a hash message algorithm of the user identification. The value is a 64 bytes message embedded within a DHCP vendor extension message field with a code of 231, which forms the secured information. As mentioned earlier, the secured information is a configuration parameter

obtained from the user (11) and the user's device, which the configuration parameter comprise one or a combination of user identification and device identification. The user identification is obtained by prompting the user (11) with the insertion of a key configuration, or in other words, a password. The device
5 identification is one or a combination of serial number or international mobile subscriber identity (IMSI) of the device. The serial number may also be a hard disk serial number.

Upon receiving the message from the user (11), the server (12) determines
10 whether the secured information is in the message (22). If so, the server (12) extracts Media Access Control (MAC) address of the device and uses the address as a key to locate the access information. The access information is obtained from the storage database (13) (23) where the access information is used as a decryption key to decrypt the secured information (24) provided by the
15 user (11). Upon decrypting the secured information, the server (12) parses the decrypted secured information and conducts a check in the storage database (13) to determine whether the decrypted secured information matches the access information. If so, the server (12) will respond to the user (11) by providing access into the network to the user (11) (25).

20

The invention described herein is susceptible to variations, modifications and/or additions other than those specifically described and it is to be understood that the invention includes all such variations, modifications and/or additions which fall within the scope of the following claims.

25

CLAIMS

1. A system (1) for accessing a network comprising:
 - at least a user (11) that requires access into a network;
 - at least a server (12) that allows the user (11) to access the network based
 - 5 on access information of the server (12) and a secured information provided by the user (11);
 - at least a storage database (13) for receiving and storing the access information and the secured information;
 - characterized in that the user (11) provides the secured information to the
 - 10 server (12) in a message in order for the server (12) to identify and decrypt the secured information based on the access information and provides access into the network to the user (11) when the secured information is decrypted.
2. A system (1) according to claim 1, wherein the user (11) is a Dynamic Host
- 15 Client Protocol (DHCP) client user.
3. A system (1) according to claim 1, wherein the server (12) is a Dynamic Host Client Protocol (DHCP) server.
- 20 4. A system (1) according to claim 1, wherein the message is a Dynamic Host Client Protocol (DHCP) message.
5. A system (1) according to claim 1, wherein the secured information is a configuration parameter obtained from the user (11) and the user's device.
- 25 6. A method (2) for accessing a network comprising the steps of:
 - sending a message to a server (12) by a user (11) to request access into a network (21);
 - determining whether there is a secured information in the message
 - 30 provided by the user (11) (22);
 - obtaining access information from the storage database (13) when the server (12) determines that the secured information is in the message (23);

decrypting the secured information using the access information obtained from the storage database (13) (24); and

providing access into the network to the user (11) when the secured information is decrypted by the server (12) (25).

5

7. A method (2) according to claim 6, wherein the user (11) is a Dynamic Host Client Protocol (DHCP) client user.

8. A method (2) according to claim 6, wherein the server (12) is a Dynamic
10 Host Client Protocol (DHCP) server.

9. A method (2) according to claim 6, wherein the message is a Dynamic Host Client Protocol (DHCP) message.

15 10. A method (2) according to claim 6, wherein the secured information is a configuration parameter obtained from the user (11) and the user's device.

1/2

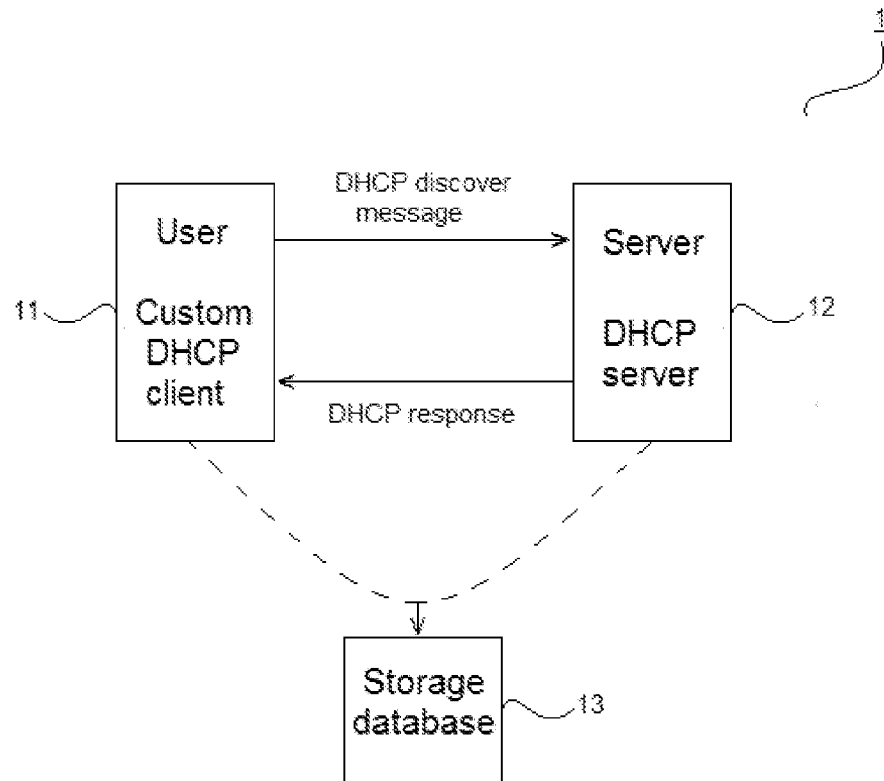
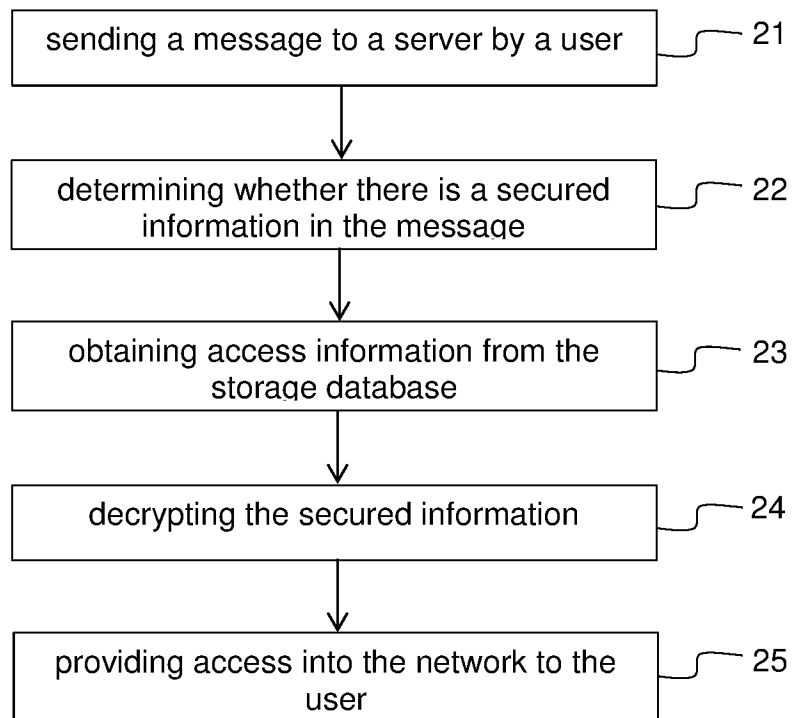


Figure 1

2/2

2**Figure 2**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/MY2015/050028

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L9/32 (2006.01) i, G06F21/44 (2013.01) i

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)

Int.Cl. H04L9/32, G06F21/44

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

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2015
 Registered utility model specifications of Japan 1996-2015
 Published registered utility model applications of Japan 1994-2015

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-326696 A (NEC CORPORATION) 2001.11.22, paragraphs [0016]-[0027], Figs. 1-2 (No Family)	1-10
Y	JP 10-242957 A (HITACHI SOFTWARE ENGINEERING CO., LTD.) 1998.09.11, paragraphs [0034]-[0036] (No Family)	1-10



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

09.09.2015

Date of mailing of the international search report

29.09.2015

Name and mailing address of the ISA/JP

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan

Authorized officer

UCHIDE, Yoshinao

Telephone No. +81-3-3581-1101 Ext. 3546

5S

4 4 4 0