(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 July 2011 (28.07.2011)

PCT

(10) International Publication Number
WO 2011/090432 A1

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/SG2010/000013

(22) International Filing Date:
19 January 2010 (19.01.2010)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **T-DATA SYSTEMS (S) PTE LTD** [SG/SG]; 1 Palm Drive, Singapore 456458 (SG).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **TAN, Joon Yong, Wayne** [SG/SG]; T-Data Systems (S) Pte. Ltd., 1 Palm Drive, Singapore 456458 (SG).

(74) Agent: **CALLINAN, Keith, William**; Marks & Clerk Singapore LLP, Tanjong Pagar, P.O. Box 636, Singapore 910816 (SG).

(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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

(54) Title: PORTABLE MEMORY DEVICE WITH AUTHENTICATION AND AUTHENTICATION METHOD AND SYSTEM

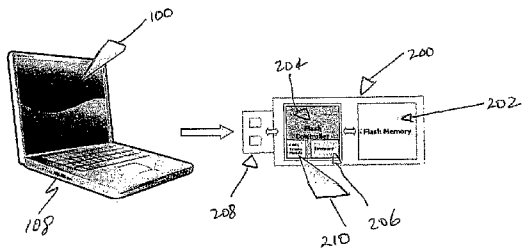

FIG. 1

(57) Abstract: A method to secure an authentication process for a portable memory device operatively connected to a host computer is disclosed. The method includes an encryption module of the portable memory device generating a unique code and sending it to a login software module of the host computer. The login software module encrypts the unique code and sends the encrypted unique code and a password to the encryption module. The encryption module decrypts the encrypted code to obtain the code for validation, and authenticates the password. A corresponding system and a portable memory device are also disclosed.

WO 2011/090432 A1

Portable Memory Device with Authentication and Authentication Method and System

Technical Field

This invention relates to a portable memory device with authentication and an authentication method and system; and relates particularly, though not exclusively, to such a device, method and system to secure an authentication process.

Definitions

Throughout this specification a reference to encryption and its grammatical equivalents is to be taken as including a reference to hashing and its grammatical equivalents; and vice versa.

Background

When using a portable memory device able to be used with a host computer by a USB connection, authentication of the user may be required when secure data is involved. Security of the authentication process may be required if there is a possibility of a "sniffing" of the password and/or a replay attack.

Summary

According to a first exemplary aspect there is provided a method to secure an authentication process for a portable memory device operatively connected to a host computer. The method includes an encryption module of the portable memory device generating a unique code and sending it to a login software module of the host computer. The login software module encrypts the unique code and sends the encrypted unique code and a password to the encryption module. The encryption module decrypts the encrypted code to obtain the code for validation, and authenticates the password.

According to a second aspect there is provided a system to secure an authentication process for a portable memory device operatively connectable to a host computer. The portable memory device comprises an encryption module and the host computer comprising a login software module. The encryption module is configured to generate a unique code and send it to the login software module. The login software module is configured to encrypt the unique code and send the encrypted unique code and a password to the encryption module. The encryption module is further configured to decrypt the encrypted code to obtain the code for validation, and to authenticate the password.

According to a third aspect there is provided a portable memory device configured to be operatively connected to a host computer. The portable memory device comprises an encryption module configured to generate a unique code and send the unique code to a login software module of the host computer. The encryption module is further configured to receive from the login software module an encryption of the unique code and a password, and to decrypt the encrypted code to obtain the code for validation, and also to authenticate the password

For all aspects the password may be encrypted or hashed by the login software module before being sent to the encryption module. The encryption or hashing of the password may be by use of the code or a derivative of the code. The login software module may establish a secure communication channel between the login software module and the encryption module before the encryption module generates the unique code. All communication between the login software module and the encryption module may be over the secure communication channel. The unique code may be selected from: a number, a series of letters, a series of numbers, characters, or any combination of them. The unique code may be used for the one communication session. A different unique code may be generated for each communication session. Encryption may comprise hashing and decryption may comprise unhashing.

Brief Description of the Drawings

In order that the invention may be fully understood and readily put into practical effect there shall now be described by way of non-limitative example only exemplary embodiments, the description being with reference to the accompanying illustrative drawings.

In the drawings:

Figure 1 is a schematic view of an exemplary system of a portable memory device connectable to a host apparatus to enable authentication of a user;

Figure 2 is a block diagram illustrating the exemplary portable memory device and a part of the host apparatus of Figure 1;

Figure 3 is flow chart for the operation of the exemplary embodiment of Figures 1 and 2; and

Figure 4 is a flow chart illustrating an additional process to that of Figure 3.

Detailed Description of the Exemplary Embodiments

To refer to Figures 1 and 2 there is shown a host computer 100 to which is operatively connectable a portable memory device 200.

The host computer 100 may be of any suitable form such as, for example, desktop computer, personal computer, laptop computer, notebook computer, server, tablet computer, personal digital assistant, digital diary, or mobile/cellular telephone.

The connection of the portable memory device 200 with the host computer 100 may be direct or indirect. If direct it may be by the USB connector 208 of the portable memory device 200 engaging with a USB port 108 of the host computer 100. If indirect, it may be by any suitable wireless connection such as Bluetooth or WiFi; or by use of a cable (not shown).

The portable memory device 200 has the USB connector 208 and a USB interface 212 operatively connected to a controller 204. A memory module 202 is also operatively connected to the controller 204. The memory module 202 may, for example, be a flash memory module. However, it may be of any suitable form of non-volatile memory.

Also operatively connected to, or integral with, the controller 204 is a firmware module 206.

Also operatively connected to, or integral with, the controller 204 is an encryption module 210.

The operation is shown in Figures 3 and 4. When the portable memory device 200 is operatively connected with host computer 100 (301), a login software module 110 in the host computer 100 establishes a secure channel 300 with the encryption module 210 of the portable memory device 200 (302). This may be by any suitable and known secure channel communication system. The secure channel 300 provides a first level of protection against "sniffing" of the password over the communication channel, and thus the possibility of a replay attack as all communication between the login software module 110 and the encryption module 210 is over the secure communications channel 300.

To further secure the user authentication process a one-time password challenge is used. For this the encryption module 210 generates a unique challenge code (303). The code may be a number, a series of letters, a series of numbers, characters, or any combination of them. The code is used for the one communication session. A different code is generated for each communication session.

The code is sent by the encryption module 210 to the login software module 110 of the host computer 100 over the secure communications channel 300. Upon receiving the code the login software module 110 encrypts or hashes the code to obtain an encrypted or hashed code (304).

The login software module 110 of the host computer 100 uses the secure communication channel 300 to send the encrypted or hashed code and the password of a user of the host computer 100 to the encryption module 210 (305).

When the encryption module 210 receives the encrypted or hashed code and the password, it decrypts or unhashes the encrypted or hashed code to obtain the code to thus provide validation (306), and authenticates the password (307). This prevents a replay attack. If the validation is not successful (i.e. the code after decryption or unhashing is not the same as the code before encryption) and/or if the password is not authenticated, the secure communication channel 300 is closed and the session ends.

Figure 4 shows a variation where following (304) the login software module 110 also hashes or encrypts the password (405) with the code or a derivative of the code. The hashed or encrypted password is then sent with the encrypted or hashed code to the encryption module 210 over the secure channel 300 (406). The encryption module 210 then decrypts the code and the password (407), validates the code and authenticates the password (409). This provides an additional layer of protection against a replay attack.

Whilst the foregoing description has described exemplary embodiments, it will be understood by those skilled in the technology concerned that many variations in details of design, construction and/or operation may be made without departing from the present invention.

The Claims:

1. A method to secure an authentication process for a portable memory device operatively connected to a host computer, the method comprising:

an encryption module of the portable memory device generating a unique code and sending it to a login software module of the host computer;

the login software module encrypts the unique code and sends the encrypted unique code and a password to the encryption module;

the encryption module decrypts the encrypted code to obtain the code for validation; and

the encryption module authenticates the password.

2. A method as claimed in claim 1, wherein the password is encrypted or hashed by the login software module before being sent to the encryption module.

3. A method as claimed in claim 2, wherein the encryption or hashing of the password is by use of the code or a derivative of the code.

4. A method as claimed in any one of claims 1 to 3, wherein the login software module establishes a secure communication channel between the login software module and the encryption module before the encryption module generates the unique code.

5. A method as claimed in claim 4, wherein all communication between the login software module and the encryption module is over the secure communication channel.

6. A method as claimed in any one of claims 1 to 5, wherein the unique code is selected from the group consisting of: a number, a series of letters, a series of numbers, characters, or any combination of them.

7. A method as claimed in any one of claims 1 to 6, wherein the unique code is used for the one communication session.

8. A method as claimed in any one of claims 1 to 7, wherein a different unique code is generated for each communication session.

9. A method as claimed in any one of claims 1 to 8, wherein encryption comprises hashing, and decryption comprises unhashing.

10. A system to secure an authentication process for a portable memory device operatively connectable to a host computer, the portable memory device comprising an encryption module and the host computer comprising a login software module; the encryption module being configured to generate a unique code and send it to the login software module; the login software module being configured to encrypt the unique code and send the encrypted unique code and a password to the encryption module; the encryption module being configured to decrypt the encrypted code to obtain the code for validation and to authenticate the password.

11. A system as claimed in claim 10, wherein the login software module is configured to encrypt the password or obtain a hash of the password before being sent to the encryption module.

12. A system method as claimed in claim 11, wherein the encryption or hashing of the password is by use of the code or a derivative of the code.

13. A system as claimed in any one of claims 10 to 12, wherein the login software module is configured to establish a secure communication channel between the login software module and the encryption module before the encryption module generates the unique code.

14. A system as claimed in claim 13, wherein all communication between the login software module and the encryption module is over the secure communication channel.

15. A system as claimed in any one of claims 10 to 14, wherein the unique code is selected from the group consisting of: a number, a series of letters, a series of numbers, characters, or any combination of them.

16. A system as claimed in any one of claims 10 to 15, wherein the unique code is used for the one communication session.

17. A system as claimed in any one of claims 10 to 16, wherein a different unique code is generated for each communication session.

18. A system as claimed in any one of claims 10 to 17, wherein encryption comprises hashing, and decryption comprises unhashing.

19. A portable memory device configured to be operatively connected to a host computer, the portable memory device comprising:

an encryption module configured to generate a unique code and send the unique code to a login software module of the host computer;

the encryption module being further configured to receive from the login software module an encryption of the unique code and a password, and to decrypt the encrypted code to obtain the code for validation and also to authenticate the password.

20. A portable memory device as claimed in claim 19, wherein the unique code is selected from the group consisting of: a number, a series of letters, a series of numbers, characters, or any combination of them.

21. A portable memory device as claimed in claim 19 or claim 20, wherein the unique code is used for the one communication session.

22. A portable memory device as claimed in any one of claims 19 to 21, wherein a different unique code is generated for each communication session.

23. A portable memory device as claimed in any one of claims 19 to 22, wherein encryption comprises hashing, and decryption comprises unhashing.

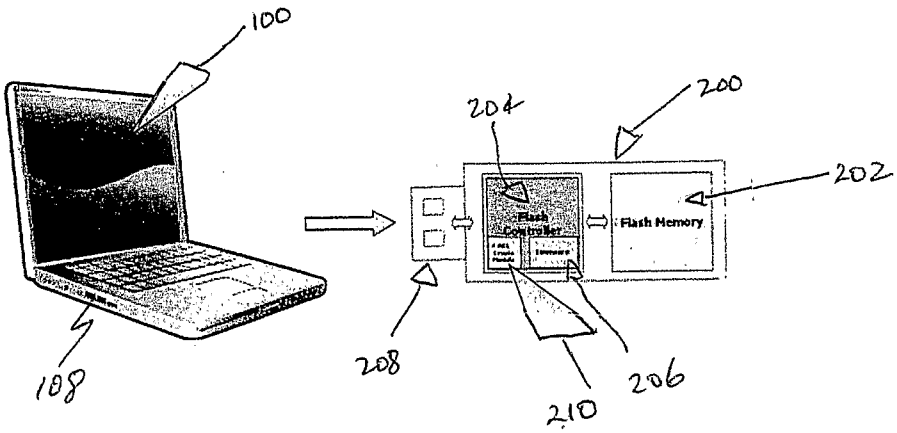
100
204
200
202
Flash Memory
208
206
210
108

FIG. 1

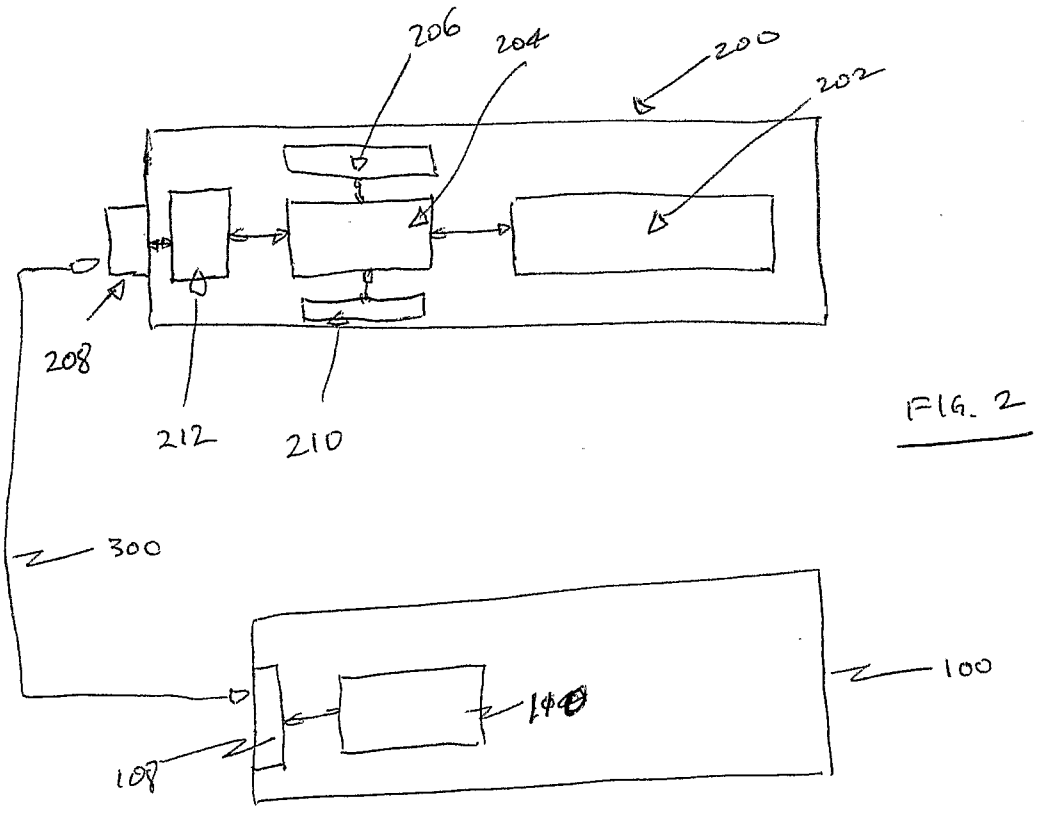
206
204
200
202
208
212
210
300
100
108

FIG. 2

2/2

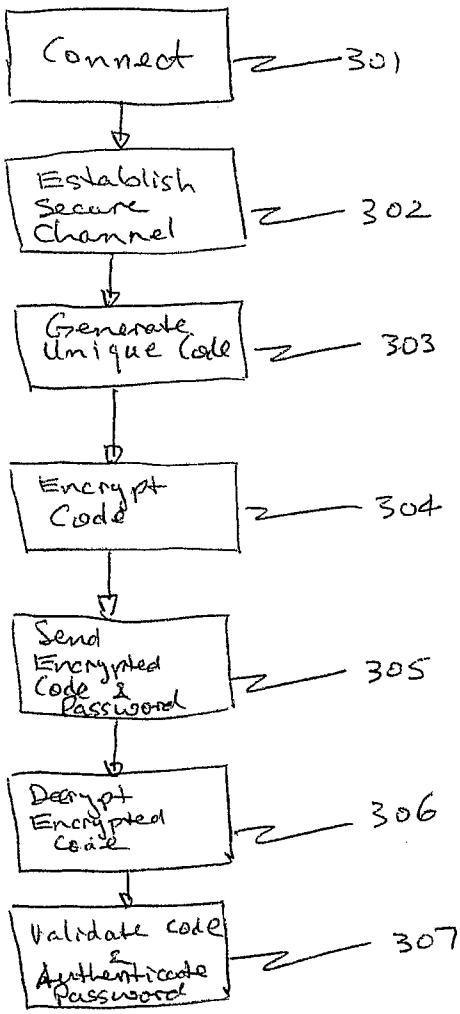
Connect
301
Establish Secure Channel
302
Generate Unique Code
303
Encrypt Code
304
Send Encrypted Code & Password
305
Decrypt Encrypted Code
306
Validate code & Authenticate Password
307

FIG. 3

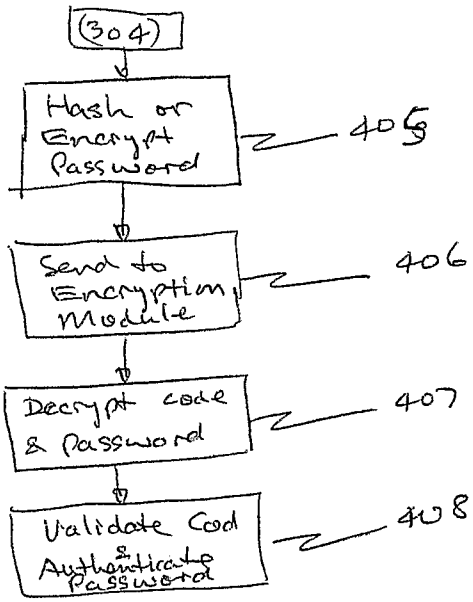
304
Hash or Encrypt Password
405
Send to Encryption Module
406
Decrypt code & Password
407
Validate Cod & Authenticate Password
408

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2010/000013

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 9/00 (2006.01) ***H04L 9/32*** (2006.01)

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)

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPOQUE and WPI searched with keywords authenticate, usb, portable memory device, crypt, hash, computer, password, code and similar terms.
Google, Google Patents, Google Scholar, and PatentScope searched with similar terms as above.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/0250473 A1 (BROWN et al.) 10 November 2005 See figure 4, paragraphs 0063-0066, and 0083.	1-23
A	US 2009/0193511 A1 (NOE et al.) 30 July 2009 See the whole document.	
A	US 7139915 B2 (DETREVILLE) 21 November 2006 See the whole document.	

☐ 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	Date of mailing of the international search report
19 February 2010	- 5 MAR 2010
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **Dr. RASIKA PERERA** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : +61 2 6283 3116

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG2010/000013

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	2005250473	CA	2530944	CN	1816997	EP	1743447
		US	7603556	US	2009240943	WO	2005/107130
US	2009193511	WO	2009/097260				
US	7139915	US	6327652	US	6330670	US	6609199
		US	6820063	US	7010684	US	7174457
		US	7194092	US	7302709	US	7356682
		US	7415620	US	7424606	US	7434263
		US	7457412	US	7529919	US	7543336
		US	2003194094	US	2003196085	US	2003196099
		US	2003196110	US	2003196111	US	2004015694
		US	2005060549	US	2005289067	US	2006021064
		US	2006036851	US	2007104329	US	2007118738
		US	2007118769				

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX