US005638444A

United States Patent [19]

Chou et al.

[11] Patent Number: 5,638,444

[45] Date of Patent: Jun. 10, 1997

[54] **SECURE COMPUTER COMMUNICATION METHOD AND SYSTEM**

[75] Inventors: **Wayne W. Chou**, Ridgefield; **Joseph M. Kulinets**, Stamford, both of Conn.

[73] Assignee: **Software Security, Inc.**, Darien, Conn.

[21] Appl. No.: **460,131**

[22] Filed: **Jun. 2, 1995**

[51] **Int. Cl.**[6] **H04L 9/08**

[52] **U.S. Cl.** **380/21**; 380/25

[58] **Field of Search** 380/4, 21, 24, 380/25

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,223,403	9/1980	Konheim et al.	380/25
4,649,233	3/1987	Bass et al.	380/21
4,906,828	3/1990	Halper	380/24
5,056,140	10/1991	Kimbell	380/23
5,144,667	9/1992	Pogue, Jr. et al.	380/45
5,148,578	9/1992	Matyas et al.	380/21
5,182,770	1/1993	Medveczky et al.	380/4
5,280,527	1/1994	Gullman et al.	380/25
5,483,596	1/1996	Rosenow et al.	380/21
5,515,441	5/1996	Faucher	380/21

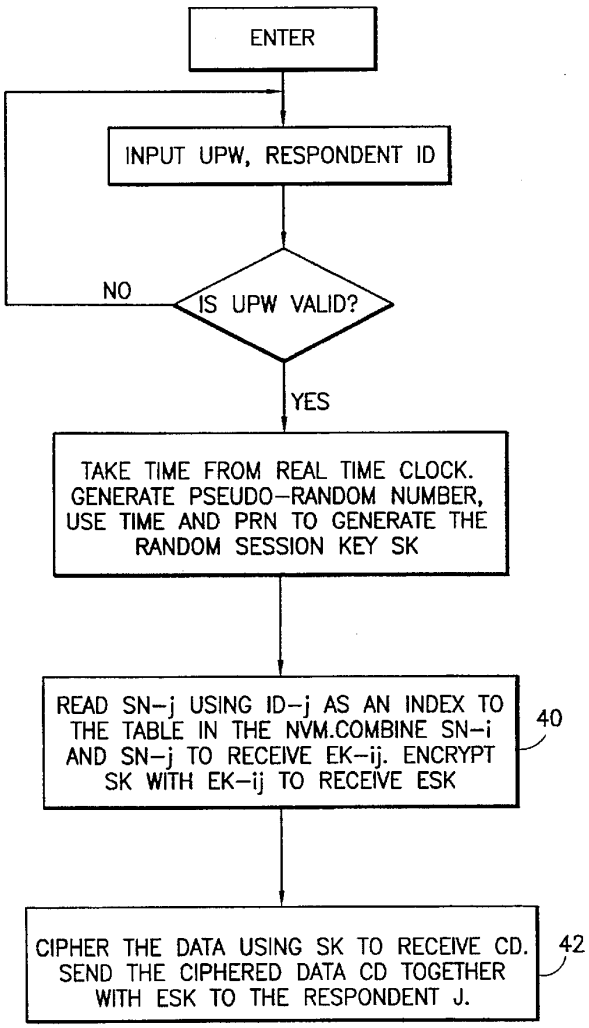
Primary Examiner—Salvatore Cangialosi

Attorney, Agent, or Firm—Parmelee, Bollinger & Bramblett

[57] **ABSTRACT**

Communication between a plurality of computers which are intercoupled or networked is provided in confidential form using password protection in combination with a special hardware token which is used to generate a one-time random session ciphering key.

5 Claims, 3 Drawing Sheets



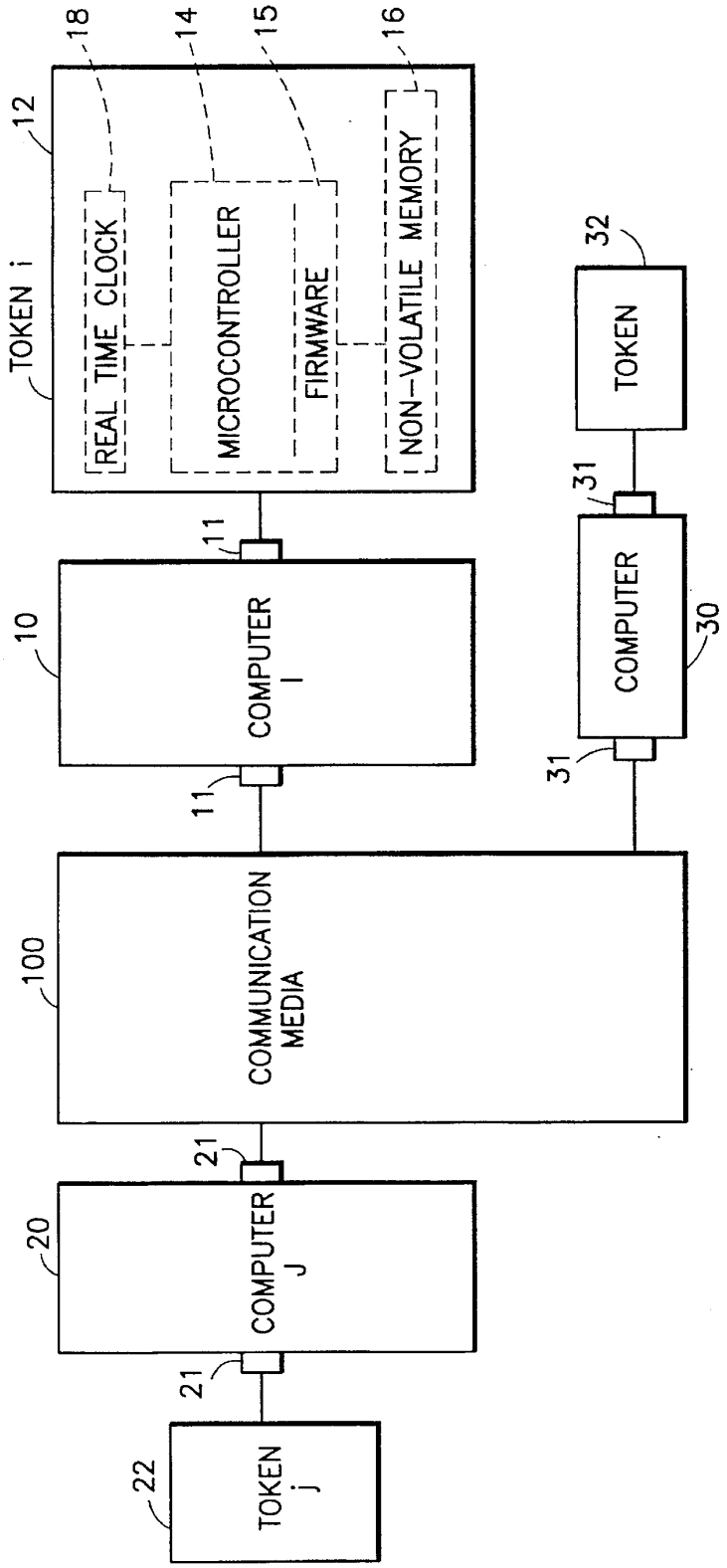


FIG. 1

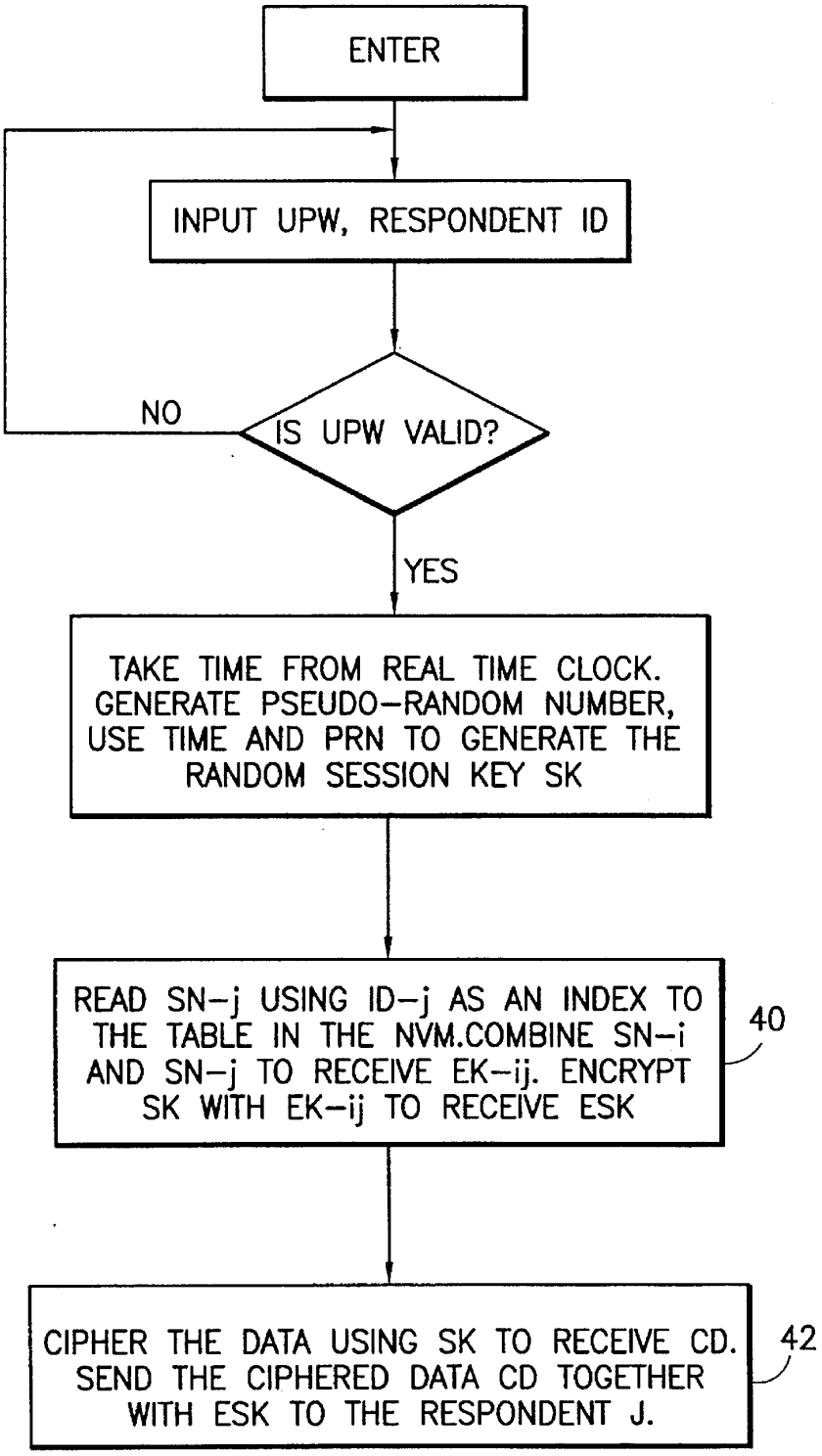


FIG. 2

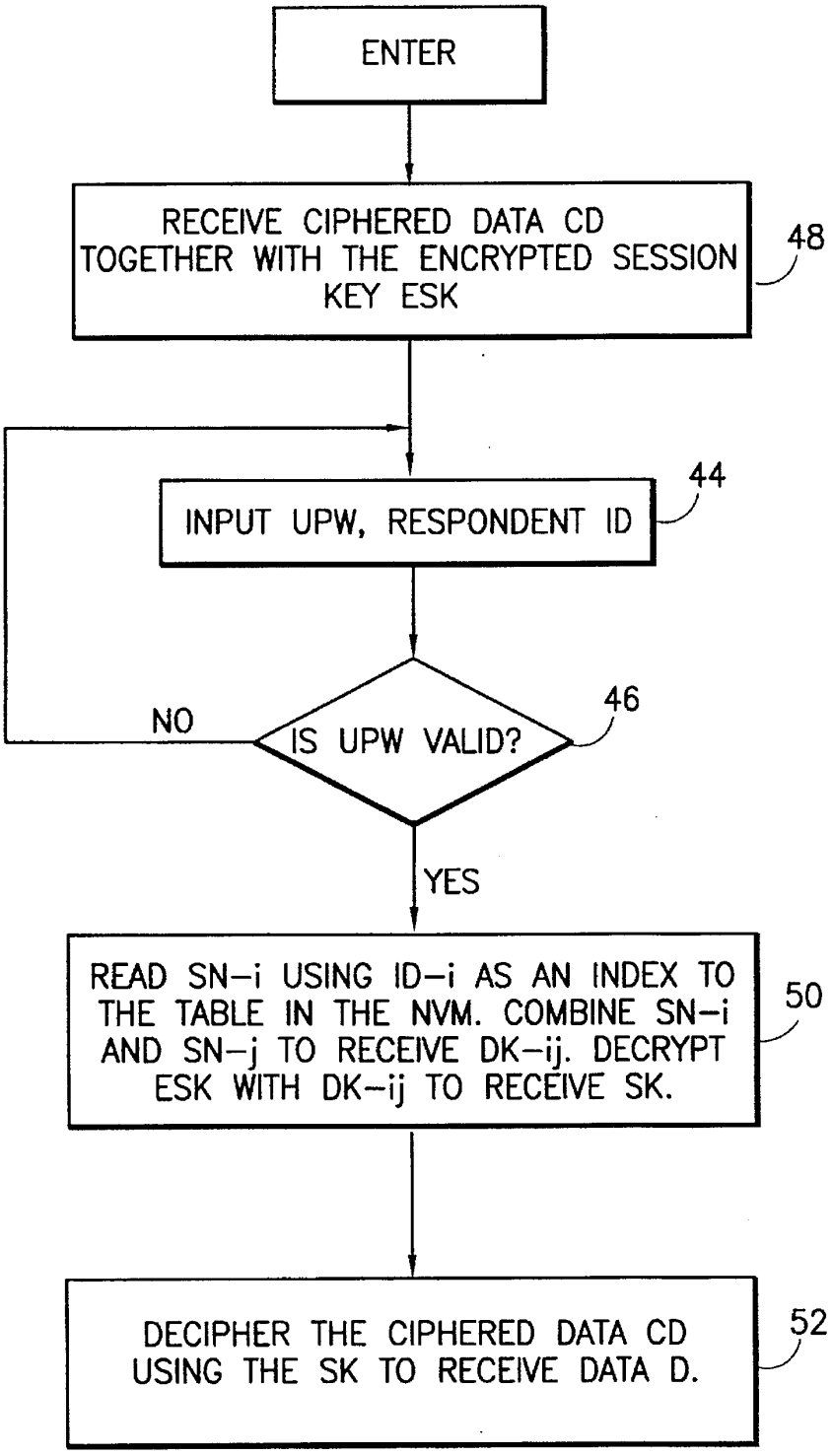


FIG. 3

SECURE COMPUTER COMMUNICATION METHOD AND SYSTEM

BACKGROUND OF THE INVENTION

This invention relates to a method and apparatus for providing secure and ciphered communications between any type of computer, including laptops and palmtops, using one-time random session ciphering keys. The method is based on password protection in combination with a special hardware device—token used for secure generation of one-time random session ciphering keys.

With the advent of more personal information sharing, electronic mail, commercial transactions and the like taking place on-line, in many instances it is desirable to protect such information transfers. Encryption methods incorporated in the computers per se are vulnerable to computer hackers when access to such computers is available.

SUMMARY OF THE INVENTION

Accordingly, it is an object of this invention to provide a new and improved method and apparatus of providing secure communications between intercoupled computers.

In carrying out this invention in one illustrative embodiment thereof, a ciphered communications method between users through their interconnected computers is provided comprising the steps of connecting hardware tokens to each computer, each token having an unduplicated and unalterable serial number incorporated therein, selecting secret user passwords and storing said passwords in non-volatile memories inside each token, creating a table inside each hardware token that lists the serial numbers for tokens of all possible respondents in the communication system together with their identification numbers, generating a random session key inside the first token belonging to the first user who wishes to start the ciphered communication as a response to a valid first user password, deriving an encryption key inside the first token based on said unique first token serial number in combination with a unique second token serial number, where the second token serial number is received from said table in response to the identification number of a respondent, encrypting a random session key using said encryption key, supplying the encrypted session key together with the unencrypted session key to the first computer where the unencrypted session key is used as a ciphering key for ciphering the data to be transmitted securely, and transmitting said enciphered data together with the encrypted session key to the recipient computer. The above method further comprises the steps of the reception of the enciphered data together with the encrypted session key by the recipient, supplying the encrypted session key to said second hardware token together with the identification number of first user who transmitted the enciphered data, deriving a decryption key inside the second token based on the unique second token serial number in combination with the unique first token serial number, where the first token serial number is received from the table of the recipient in response to the identification number of first user and to a valid second user password, decrypting the encrypted session key inside the second token using said decryption key, transmitting the decrypted session key to the second computer and deciphering the ciphered data with the session key.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention together with further objects, features, aspects and advantages will be more clearly understood from the following description taken in connection with the accompanying drawings.

FIG. **1** is a block diagram of the secure computer communication system in accordance with the present invention;

FIG. **2** is a flow chart illustrating secure communication from a sending computer to a receiving computer; and

FIG. **3** is a flow chart illustrating the deciphering process at the receiving computer.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to FIG. **1**, a computer network of intercoupled computers **10**, **20**, **30**, etc. via computer ports **11**, **21** and **31**, respectively, and communication media **100** such as a network (LAN, WAN, wireless, etc.) or communication channels including modems is illustrated to permit secure ciphered communications between computers in accordance with the present invention. The ciphered communications is based on the use of a one-time session enciphering key derived and encrypted inside the hardware token, transferred to the respondent together with the enciphered message and decrypted inside the respondent hardware token together with the password protection of all the operations inside hardware tokens.

Each hardware token **12**, **22**, **32**, etc., for example, as is illustrated in connection with the token **12**, includes a programmed microcontroller **14** with the incorporated firmware programs **15**, that cannot be read outside the token, a non-volatile memory **16**, unduplicated and unalterable serial number, that can be stored in a non-volatile memory **16** or be incorporated into firmware **15**, and a real time clock **18**. Non-volatile memory **16** retains all the data written even after the power for the hardware token is cut off.

The firmware **15** inside the microcontroller **14** performs the functions of a random number generator using the random input from the real-time clock **18**.

Each user of the system operating from the respective computer **10**, **20**, **30**, etc. chooses a user password that is stored in the respective non-volatile memory **16** of hardware token **12**, **22**, **32**, etc. connected to each computer **10**, **20**, **30**, etc. Inside the non-volatile memory **16** of each token, there is a special table which contains the identification numbers of all the possible respondents for this user in the communications system, thereby providing an index for the entry of the respective serial numbers of all the respondents hardware tokens. Accordingly, before the actual secure communication takes place, the users of hardware tokens **12**, **22**, **32**, etc. will exchange their serial numbers which are entered into their respective hardware tokens together with the established identification numbers. For each possible respondent to securely communicate with a given user, the user's hardware token must contain an entry in the above table having the identification number and serial number of the hardware token of the respondent with whom communication is to be conducted.

Security in accordance with the present invention is based on using constantly changing one-time session keys for each communication session between any pair of users or for a part of such a communication session. The generation of the session key is accomplished inside the hardware token of the user, who initiates the communication which, in this illustrated example, is token **12**. The session key (SK) is generated by microcontroller **14** based on a constantly changing output of a pseudo-random number (PRN) generator and a secret algorithm in the microcontroller **14** implemented in the firmware **15** of the microcontroller **14** together with the

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.