US 20080282360A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2008/0282360 A1

(43) Pub. Date: Nov. 13, 2008

BAHAR

(54) ACTIVATION CODE SYSTEM AND METHOD FOR PREVENTING SOFTWARE PIRACY

(76) Inventor: **REUBEN BAHAR**, West Hills, CA (US)

Correspondence Address:
MARVIN A. GLAZER
2141 E. HIGHLAND AVE, SUITE 155
PHOENIX, AZ 85016 (US)

(21) Appl. No.: **12/182,135**

(22) Filed: **Jul. 30, 2008**

Related U.S. Application Data

(60) Continuation of application No. 11/311,964, filed on Dec. 19, 2005, which is a division of application No. 09/594,004, filed on Jun. 14, 2000, now Pat. No. 7,024, 696.

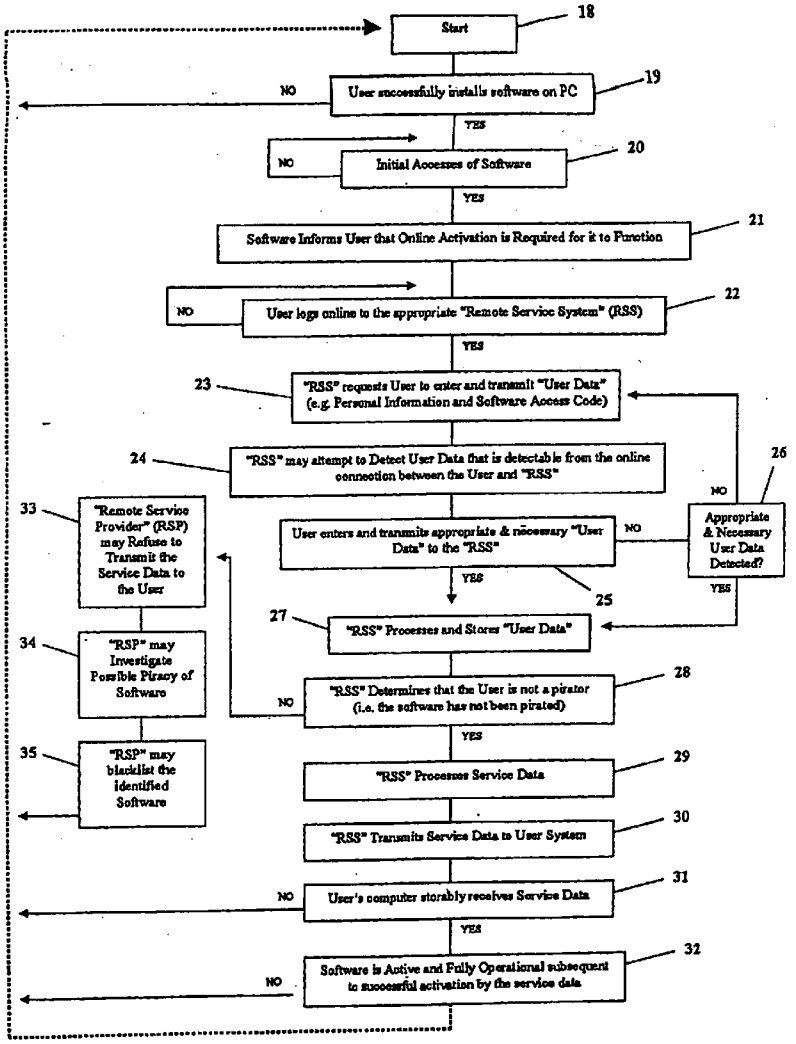
Publication Classification

(51) **Int. Cl.**
G06F 21/24 (2006.01)

(52) **U.S. Cl.** **726/30**; 726/31

(57) **ABSTRACT**

A system and method for preventing piracy of a given software application limits the number of times that such software application is activated. A given software application must be activated in order to become fully functional. The user must provide a unique software identification code, relating to the specific software which the user is attempting to activate, to a remote provider. The remote provider determines the number of times that such specific software has already been activated, and provides an activation code to the user unless the number of activations exceeds a predetermined threshold. Once activated, the software becomes fully operational, and the user is allowed complete access to its functions.



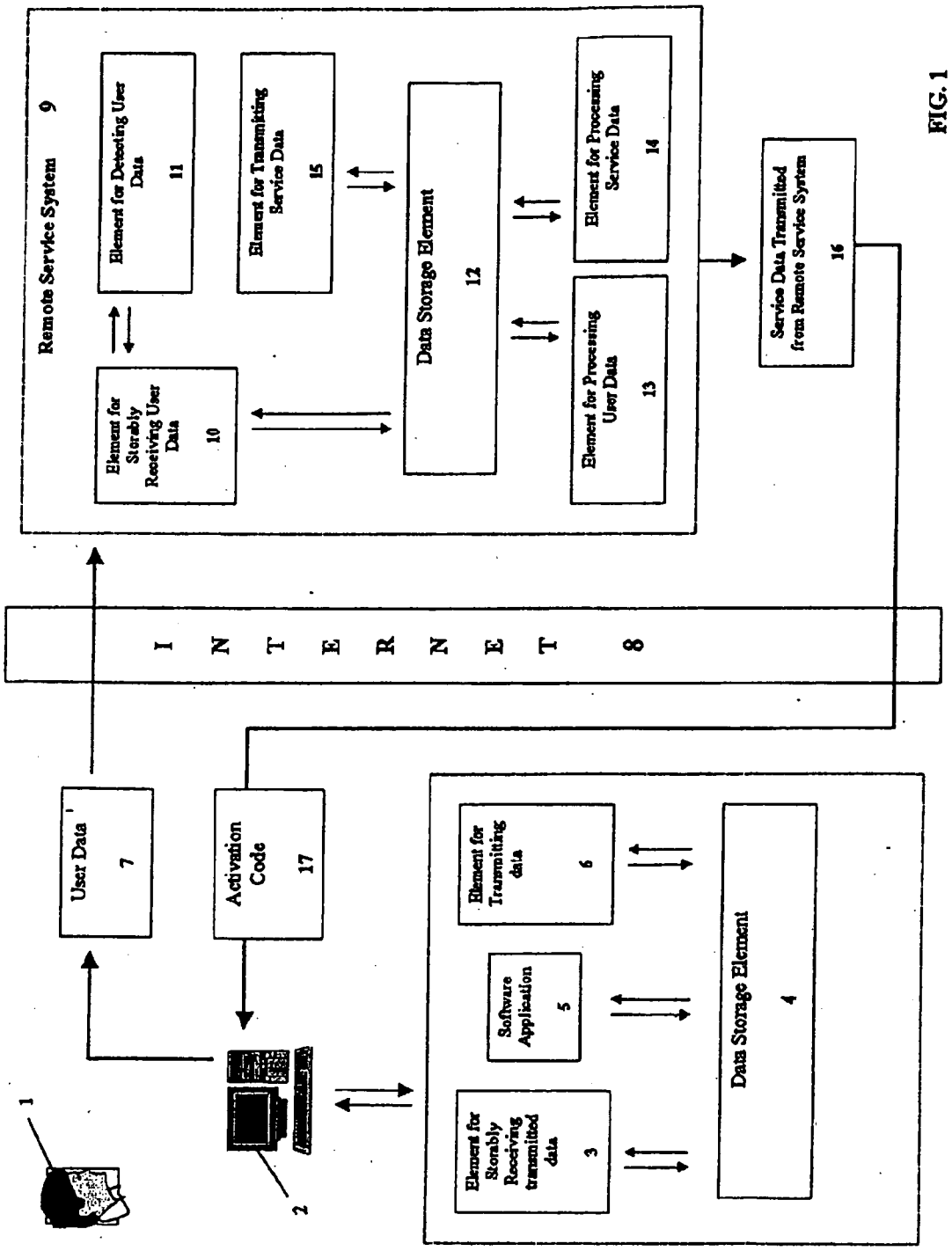


FIG. 1
Method 100

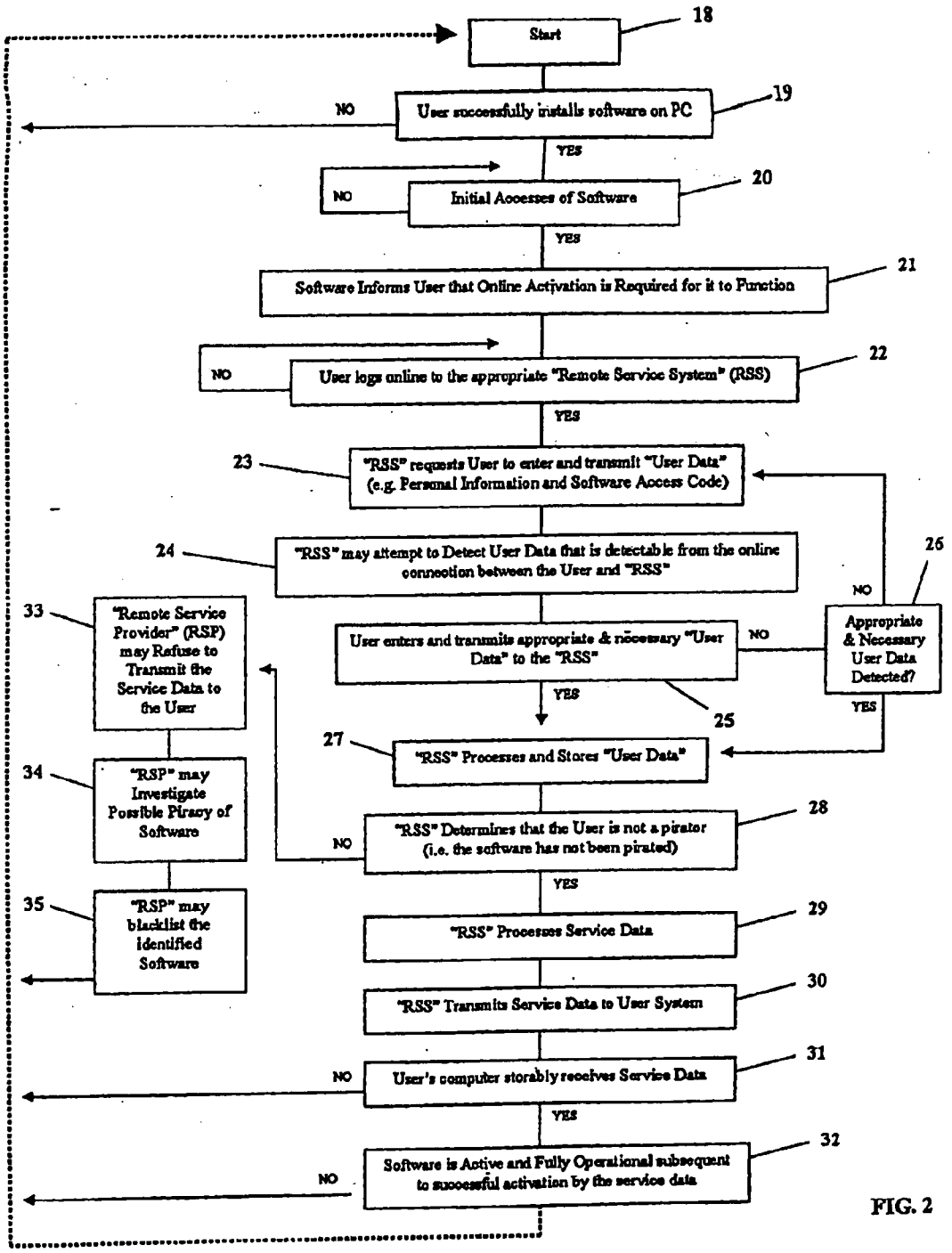

Start
18
User successfully installs software on PC
19
NO
YES
Initial Accesses of Software
20
NO
YES
Software Informs User that Online Activation is Required for it to Function
21
User logs online to the appropriate "Remote Service System" (RSS)
22
NO
YES
"RSS" requests User to enter and transmit "User Data" (e.g. Personal Information and Software Access Code)
23
"RSS" may attempt to Detect User Data that is detectable from the online connection between the User and "RSS"
24
User enters and transmits appropriate & necessary "User Data" to the "RSS"
25
NO
YES
Appropriate & Necessary User Data Detected?
26
NO
YES
"RSS" Processes and Stores "User Data"
27
"RSS" Determines that the User is not a pirator (i.e. the software has not been pirated)
28
NO
YES
"RSS" Processes Service Data
29
"RSS" Transmits Service Data to User System
30
User's computer storably receives Service Data
31
NO
YES
Software is Active and Fully Operational subsequent to successful activation by the service data
32
NO
"Remote Service Provider" (RSP) may Refuse to Transmit the Service Data to the User
33
"RSP" may Investigate Possible Piracy of Software
34
"RSP" may blacklist the identified Software
35

FIG. 2

ACTIVATION CODE SYSTEM AND METHOD FOR PREVENTING SOFTWARE PIRACY

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This patent application is a continuation of co-pending U.S. patent application Ser. No. 11/311,964, filed Dec. 19, 2005, which is a divisional application based upon prior-filed U.S. patent application Ser. No. 09/594,004, filed Jun. 14, 2000, now U.S. Pat. No. 7,024,696, and the benefit of such earlier filing dates is hereby claimed by Applicant under 35 U.S.C. § 120.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The field of the invention generally relates to methods for preventing the piracy of software applications. The invention relates more particularly to a computer method and system for preventing the piracy of a given software application through use of a communications network, such as the Internet, wherein a given software application, installed on a user system, will function only after a remote service provider transmits a code sequence that will activate the software for use.

[0004] 2. Description of the Related Art

[0005] The creation of the personal computer has drastically simplified the way in which people manage their business and personal affairs. One of the main reasons why the computer has had such a great impact on our lives is due to the constant development of software applications which allow the computer to perform an array of different tasks and functions. As software applications advance, however, so too does their complexity and the programming skill needed to write and develop them. This has naturally caused many software applications to be quite expensive. Such high costs have often resulted in unauthorized distribution of copied software that has not been paid for or licensed to the user. This type of piracy is especially common among friends, relatives, and business associates. Additionally, people also profit from piracy by producing illegal copies of a software application and distributing them in mass quantities for drastically reduced prices.

[0006] Due to the availability and low cost of sophisticated computer equipment such as the CD Write/Re-Write drive, software piracy has become a much greater concern over the current years. Today, virtually everyone can get access to such equipment and distribute CD based copies of software applications to whomever they please. Mass distribution of pirated software not only deprives software manufacturers of their deserved earnings, but also allows other software pirators to pirate unlicensed copies of that application and propound the damage exponentially. As such, piracy has often resulted in inflated software prices and irreparable damage to software companies.

[0007] In an effort to combat the problems of software piracy, many software companies have employed various preventative measures. Some of these include software access codes, activation plugs (i.e., Memo-HASP), registration, and even costly technical support services. Although somewhat effective, these measures have often been defeated with relative ease and little or no expense. For example, software access codes which must be entered to gain access to the software, are disclosed with the software package and are thus, easily copied and distributed to unlicensed users. Activation plugs, such as the ones which attach to the PC's parallel port, have also been easily duplicated by various manufacturers who illegally sell them on the black market. Furthermore, while registration of the software would inform the manufacturer of all users (licensed and unlicensed), pirators rarely register given the absence of a compelling motivation to do so. Lastly, technical support groups are likewise, rarely used by pirators, given their reluctance to disclose their illegal use of the software. As shown by these and other ineffective measures, it would be advantageous for a software manufacturer to control the functionality of a given software application in relation to each of its identified users.

BRIEF SUMMARY OF INVENTION

[0008] It is the object of the present invention to provide a reliable and effective method and system for preventing piracy of a given software application over a communications network, whereby the software application will not function unless activated by a remote service provider.

[0009] It is further the object of the present invention to provide a method and system for identifying each separate user of a given software application who installs and intends to effectively utilize the given software application.

[0010] It is further the object of the present invention to provide a method and system for associating user data to archived data accessible by the remote service provider, in order to determine if the user is a pirator of the software application.

[0011] Briefly described, and in accordance with preferred embodiments thereof, the present invention relates to a method and system for preventing piracy of individual software applications. A remote service system, controlled by a remote service provider, storably receives user data that is transmitted by a user of a given software application. Upon receiving the user data, the remote service system associates it to stored archive data which is accessible to the remote service provider. If it is determined that the user is not a pirator of the software, the remote service system will transmit service data which will activate the software and allow the user to utilize its full functionality. In this manner, the remote service provider can limit software piracy, as only legitimate users of the software will be given the service data needed to activate the software.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. **1** is an overview diagram pictorially illustrating the flow of information that occurs between a user of a given software application and the remote service system in a preferred embodiment of the method and system for prevention of software piracy according to the present invention.

[0013] FIG. **2** is a block flowchart of the information flow that occurs in a preferred embodiment of the method and system for prevention of software piracy according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] In reference to the drawings, FIGS. **1** and **2** show the information flow that occurs in a method and system (hereinafter "method"), indicated at reference character **100** in FIG. **1**, for preventing of piracy of a given software application via a communications network, such as the Internet **8**.

Both FIGS. **1** and **2** illustrate the process by which a user would attempt to activate a given software application.

[0015] As shown in FIG. **1**, the user **1** successfully installs a given software application **5** (hereinafter "software") on the data storage element **4** of the user's system **2**. The user system **2** is generally defined as the user's computer terminal, which typically consists of a central processing unit, or CPU (not shown), a data storage element **4**, an element for storably receiving transmitted data **3**, an element for transmitting data **6**, and a monitor and keyboard. While the software **5** may utilize various anti-piracy measures, two such measures, are especially worth noting in relation to the present invention, and are discussed in greater detail below. The first measure is a program code sequence that identifies the specific software **5** (hereinafter "identification code"), while the second is an additional program code sequence that would be needed to activate the software **5** (hereinafter "activation code"). It is preferred that transmission of both of these code sequences, between the user **1** and remote service system **9**, would be accomplished over the Internet **8**. As used herein, a "user" can be an individual entity or collaborate entity, such as a business, family, or even friends, who legitimately acquired a license and/or right to use the given software **5**. Furthermore, the remote service system **9** can be the software manufacturer or an independent company, working in conjunction with the software manufacturer, to prevent software piracy.

[0016] Upon an initial attempt to access the installed software **5**, user **1** will be informed that the software **5** requires online activation before it can be operational. Online activation will render the given software **5** operational, subject to receiving the activation code from the remote service system **9**. This requires that the software **5** be designed wherein it is either partially or completely dysfunctional prior to receiving the activation code, as will be discussed below. By connecting to the remote service system **9** through the Internet **8**, a user who is not pirating the software **5** will be able to have the software **5** activated online. Although the Internet **8** is used herein when referencing a communications network, the present invention is intended to include all forms of communications network environments known to one skilled in the relevant art. Thus, method **100** is equally applicable to all interconnected computer systems capable of transmitting and receiving data, preferably digital data, which allow users of the network to communicate. In this regard, a communications network includes, but is not limited to, all telecommunications networks such as the Internet, i.e. the World Wide Web and BBS systems, hardwire telephony, wireless networks including cellular and PCS systems, satellite networks, etc. Furthermore, communications networks include localized and regional networks such as intranets and local area network (LAN) systems which interconnect a relatively few number of user systems or terminals, typically by means of a centralized server.

[0017] Once user **1** establishes an online connection to the remote service provider **9**, user **1** enters and transmits user data **7**, via an element **6** for transmitting user data, to the remote service system **9** over the Internet **8**. The user data **7** is subsequently received by the remote service system **9** via an element **10** for storably receiving user data, and stored in the data storage element **12** of the remote service system **9**. Although the transfer of user data **7** to the remote service system **9** would preferably be initiated by user **1**, this need not always be the case. Once user **1** connects to the remote service system **9** via the Internet **8**, the user data **7** may be automatically detected by an element **11** for detecting user data of the remote service system **9**. In this case, the detected user data **7** will likewise be received by the remote service system **9** via element **10**, and subsequently stored by the data storage element **12** of the remote service system **9**. It is notable that the term "user data" is defined and understood herein and in all the claims to mean any information originating from and/or available to the user of the software **5**. This includes, but is not limited to personal identification information such as user name, address, location, phone number, etc. Additionally, user data **7** may consist of any information relating to the software **5** which identifies and distinguishes it from other "same type" or distinct software applications. This can include, but is not limited to information such as an "identification code" (as noted earlier), a product serial number, name, and/or version number.

[0018] It is worthy to mention that the software **5** should preferably contain an identification code, which is a program code sequence comprised of alphanumeric characters, that would serve to identify each authorized copy of a software application. Given its function, the identification code may be synonymous with a product's distinct serial number. Preferably, the identification code will be unique to each software application sold, and will be disclosed to both user **1** and remote service system **9**. The advantage of a unique identification code is that it will allow the remote service system **9** to recognize and keep track of each authentic copy of a software application sold. Although the identification code could consist of an elongated alphanumeric code sequence, such as a "program file(s)", it is preferred that it consist of a short code sequence of alphanumeric characters, e.g. XJR-U89K-RJ2P1. A short identification code sequence will allow the software **5** to be simply and easily identified. It should finally be noted that user data **7** may also refer to information identifying the user system **2** such as serial and model number as well as the type, function, and performance of the various system hardware components.

[0019] After receiving and storing user data **7**, the remote service system **9** processes the user data **7** via an element **13** for processing user data. Element **13** may be, but is not limited to, software, hardware device(s), or a combination of these two, which would allow for processing of the user data in the manner noted herein. Additionally, element **13**, used to process user data, may likewise include the remote service system's personnel staff who would be able to manually initiate processing of the user data, in the manner noted below.

[0020] Processing of the user data may include, but is not limited to an "archiving" event wherein a wide range of information that is received by or made available to the remote service system **9** is sorted, arranged, and organized into retrievable data files. Archived data stored in the data storage element **12** of the remote service system **9** may consist of, but is not limited to, a mass assortment of receivably stored user data (e.g. "identification codes"), service data (discussed below), and promotions, etc. Here, the archived data would relate to distinct users, various software applications, and potential advertisements; all of which may exist independently of one another. Second, archived data may also consist of information indicating the amount of user online activation attempts recorded for each identified software **5**. Finally, archived data may include all other information that might be of use to the remote service system **9** in preventing piracy of a given software application.

[0021] Processing of the user data **7** may also consist of an "associating" event wherein the currently transmitted user data **7** is compared to archived data contained in the data storage element **12** of the remote service system **9**. It is important to note that "associating" the currently transmitted user data **7** to archived data will allow the remote service system **9** to determine if the user **7** is attempting to activate a pirated version of the software **5**. Here, the "product identification code" of software **5**, along with other user data **7** currently being received from the user system **2**, will be compared to existing archived data. If the archived data establishes that the software **5** is legally registered to a completely distinct user, such may indicate that the user currently online is trying to activate a pirated version of the software **5**. This result will occur if the archived data referencing the software **5** does not match the user data **7** currently being transmitted by the user system **2**, and/or if the archived data indicates that there have been repeated and numerous attempts to activate the same software **5**.

[0022] Multiple online activation attempts of the same software **5**, regardless if such attempts are by distinct or the same users, would naturally indicate that the software **5** was pirated and distributed to a multitude of different users. In this situation, the remote service provider may contact the registered user(s) to investigate into potential piracy. Additionally, the remote service system **9** may "blacklist" the specific software **5**, as referenced by its identification code. Blacklisting of a given software application would mean that the identified software would be prohibited from receiving any future activation codes from the remote service system **9**. For all intents and purposes, such an event would render the identified software void and permanently dysfunctional. This is because the software, as sold to the user, would need the activation code in order to function. Absent this code, the identified software would be inoperative and no longer subject to piracy.

[0023] When it is determined by the remote service system **9** that user **1** is not a pirator of the software **5**, service data, such as the activation code **17**, may be transmitted to the user system **2**. The software **5** and/or the user system **2** are responsive to such service data. As used in this invention, the term "service data" is defined and understood herein and in all the claims to mean any data that the remote service system **9** may legitimately transmit to the user system **2** during the online activation process for the software **5**. Service data **16** may include, but is not limited to instructions, promotional messages, and an activation code(s). The instructions may guide user **1** through the steps for activating the software **5**, while a promotional message program code sequence may offer and display a particular product or service for sale. The activation code **17**, as noted earlier, is a program code sequence that will serve to activate each individual software application, which absent the activation code **17**, would be dysfunctional. The activation code may either be unique to each individual software **5** sold (hereinafter "unique activation code") or unique to a group of software (hereinafter "common activation code") that relate to a common software program, manufacturer, brand name, or version, etc. Of the two, the preferred embodiment would be the "unique activation code" which is unique to each individual software **5** sold.

[0024] One of the main advantages of using a unique activation code is the drastic curtailment of software piracy. Each authorized copy of software application **5** is designed to be responsive to a distinct activation code. As such, an attempt to pirate distinct software applications would entail a tedious and time consuming task requiring the hacker to uncover the activation code of each individual, authorized software product. Furthermore, a unique activation code will not allow for the activation of any "general" copy of the software which would otherwise be responsive to a common activation code. As an alternative to a unique activation code, a common activation code would activate all "same type" software applications. Developing "same type" software to be responsive to a common activation code may be advantageous given the potential for reducing confusion and troubleshooting errors which could arise during the software manufacturing and online activation stages.

[0025] It is noteworthy to mention that, similar to the identification code, the activation code may likewise consist of either a long or short program code sequence. As noted earlier, a short code sequence would consist of a concise sequence of alphanumeric characters, e.g. HT3-GY2K-WROP, while a long code sequence would consist of a small or large arrangement of alphanumeric data that result in a "program file(s)". Use of a long code sequence would be the preferred method of constructing the activation code. This is because a long code sequence (i.e. a program file) would be much harder to replicate than a short code sequence. Software application **5** can initially be supplied missing certain program files necessary for software application **5** to function. Only after these missing program files (e.g., the activation code) are transmitted from the remote service system **9** to the user system **2**, will the software **5** be functional.

[0026] An activated software application will be fully operational and allow the user complete access to it. Although not required, activation code **17** preferably remains undisclosed to user **1**. The need for the activation code will compel user **1** to register the software **5** online with the remote service system **9**. Furthermore, and more importantly, having the activation code **17** only known to the remote service provider and its business affiliates (such as the software manufacturer) will prevent piracy of the software **5**. This is because users who wish to pirate the software **5** will not be able to replicate the activation code and distribute it along with a medium (e.g. CD ROM) containing a copy of the software **5**. Activation code **17** is preferably designed to be immune from discovery by computer hackers and sophisticated programmers. The objective is to prevent these individuals from "breaking in" to the software **5** and either re-writing or discovering the undisclosed activation code. As noted earlier, this may require constructing the activation code as a long code sequence which results in a program file(s). Additionally, other measures may include code encryption as well as any other programming methods known to those skilled in the relevant technical art.

[0027] Before software application **5** can be activated, the appropriate service data must be processed and transmitted to the user system **2**. Processing of the service data **16** requires that it be either extracted or generated from the archived data stored on the data storage element **12** of the remote service system **9**. Extraction or generation of the service data **16** is accomplished by an element **14** for processing service data, as referenced in Method **100** of FIG. **1**. Element **14** may be, but is not limited to, software, hardware device(s), or a combination of the two, which would allow for processing of the service data, in the manner described herein. Additionally, element **14**, used to process service data **16**, may likewise include the remote service system's personnel staff who

would be able to manually initiate processing of the service data **16**, in the manner described herein.

[0028] Extraction of service data **16** from the archived data entails a selection process wherein only the appropriate and necessary service data is singled out from the total archived data and made available for transmission to the user system **2**. Extraction of the service data is necessary given the variety of software applications, and the multitude of distinct service data entries, that may be stored and archived by the remote service system **9**. For example, the activation code "ABC-123", contained in the archived data, would only be extracted when a user **1** who possesses the specific software referencing the identification code "ABC-123" attempts to activate it online. Stated differently, service data containing an activation code relating to Microsoft Word 2000 would not be extracted for a user trying to activate a Norton Anti-virus software application. The reason for this is that different users will require different service data, depending on the requirements of the specific software that they are attempting to activate.

[0029] Alternatively, the second embodiment for processing the service data **16** pertains to an event which causes the service data **16** to be generated. This event entails a process wherein pre-existing archived data may be formulated into the appropriate service data upon request from the remote service system **9**. Generation of service data can be advantageous, as this method will permit the remote service system **9** to manipulate various data components, existing in the archived data, in order to formulate the service data **16**. For example, the remote service system **9** may combine personal identification information belonging to user **1** with promotional data to formulate a personalized advertisement directed at user **1**. Additionally, the remote service system **9** could combine user data (such as the directory file location of the user system **2** that contains the installed software **5**) with the appropriate activation code, to formulate a self executing program file which, upon an access event, would automatically install the service data **16** into the correct file location of the user system **2**. Formulation of the service data may include, but is not limited to, a series of calculations, combinations, and/or sorting out of the appropriate archived data. Generation of the service data may occur at any time prior to or after the remote service system **9** determines that user **1** is not a pirator of software **5** and is eligible to receive the service data **16**.

[0030] Once the service data **16** is extracted or generated via element **14** (i.e., the element for processing service data), the remote service system **9** transmits service data **16** to the user system **2**. Transmission of the service data **16** may be accomplished in a number of ways. The first two methods involve an event wherein the service data **16** is uploaded into the user system **2**, while the third method requires user **1** to download the service data **16** into user system **2**. In the first embodiment for uploading the service data **16**, the remote service system **9** initiates an uploading event in which the service data is automatically transferred from the remote service system **9** to the user system **2** wherein it is storably received via storage element **3** for storably receiving service data **16**. It may be necessary for the remote service system **9** to determine the appropriate file directory location on user system **2** in which to upload the service data. Determination of this location may be accomplished by, but is not limited to, manual selection by user **1**, as transmitted by the user (e.g. user data), or via an interactive search of the file directory of user system **2**.

[0031] In the second embodiment for uploading of service data **16**, remote service system **9** manually transmits the service data **16** to the user system **2**. Manual transmission of the service data **16** allows remote service system personnel to decide when the transfer sequence should be initiated. Furthermore, manual transmission enables such personnel to manually enter and transmit needed service data **16** which may not have been processed by element **14** within remote service system **9**.

[0032] Finally, in a third embodiment, the service data **16** is made available to user **1** for downloading into user system **2**. The remote service system **9** transfers the archived data **16** into a file that can be downloaded by user **1**. The downloaded file contains service data and possibly some elements of user data. As noted earlier, it is preferred that the file contain a self-executing installation program that is triggered upon an access event by the user. For example, as a result of successfully downloading and accessing the file, service data **16** may automatically be installed into the appropriate file directory of the user system **2**.

[0033] Following successful upload or installation of the service data **16** (e.g., the activation code **17**) into the user system **2**, the software **5** will gain full functionality. Complete activation of the software **5** will allow user **1** to freely utilize it to its full potential. Preferably, user **1** will never need to go through the online activation process (as mentioned herein) again unless user **1** attempts to install the software **5** on another user system, or attempts to re-install it on current user system **2**.

[0034] Although many different scenarios can arise during the online activation process of a given software **5**, FIG. **2** illustrates, in block diagram form, one possible "real time" cycle run of the present invention. Starting from block **18**, user **1** successfully installs a given software application on user system **2**, at block **19**. Following an initial access event of the software **5**, as indicated by block **20**, the software **5** proceeds to block **21**, and informs user **1** that online activation is required in order for it to function. If user **1** decides to register the software **5**, user **1** must connect online to the appropriate remote service system **9**, as shown at block **22**. At this point, the remote service system **9** may request user **1** to enter and transmit user data **7** to the remote service system **9**, as indicated by block **23**. The remote service system **9** may also attempt to detect any user data **7** that can be detected by virtue of the online connection between the user system **2** and remote service system **9**, as represented by block **24**. If the appropriate and necessary user data **7** is entered and transmitted by user **1**, at block **25**, or detected by the remote service system **9**, at block **26**, then such user dated is stored and processed by the remote service system **9** as indicated at block **27**. It should be noted that, if user **1** fails to provide and transmit the appropriate and necessary user data **7**, and/or if remote service system **9** is unable to detect the appropriate and necessary user data **7**, the cycle will repeat and be taken back to block **23** of FIG. **2**.

[0035] The processing of user data **7** allows remote service system **9** to determine if the user is a pirator of the software **5**. If remote service system **9** determines that user **1** is not a pirator, at block **28**, then service data **16** is processed, at block **29**. At this point, remote service system **9** transmits service data **16** to user system **2**, at block **30**. Transmission may be

accomplished via uploading or downloading methods as described earlier. After service data **16** is storably received by user system **2**, at block **31**, the software **5** will be active and fully operational subject to successful activation by service data **16**, as indicated by block **32**. In the event that service data **16** is not properly received by user system **2**, or fails to activate the software **5**, the cycle will repeat, starting from block **18**.

[0036] Finally, it is noteworthy to mention that, in the event that remote service system **9** determines that user **1** is pirating the software **5**, remote service system **9** may refuse to transmit the service data **16**, as shown by block **33**. Additionally, it may investigate into the possibility of piracy, at block **34**, as well as blacklist the identified software **5**, as shown by block **35**.

[0037] The program code sequence, and all other technical aspects described above, are all conventional and known to those skilled in the art and need not be described in detail herein. Furthermore, the term "element", as stated in the specification and all the claims herein, may be construed in the singular and/or the plural tense.

[0038] The above-described embodiments of the present invention are to be considered in all respects as illustrative, and not restrictive; the scope of the invention is indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are intended to be embraced therein.

1. A computer usable medium having computer readable code comprising:

a) software that requires an activation code to activate at least part of the functionality of the software;

b) program code that requires an identification code which identifies the software;

c) program code that enables the software to receive an activation code for activating at least part of the functionality of the software, said activation code representing that the number of times that said software has been previously activated on distinct user systems in a manner that is independent of the identity of the user is less than a predetermined threshold, said predetermined threshold being at least two.

2. The computer usable medium of claim **1** wherein the program code that requires the identification code does so by requiring entry of the identification code to identify the particular copy of the software to be activated.

3. The computer usable medium of claim **1** further comprising program code that enables the particular copy of the software to initiate contact with a remote service provider and to communicate said identification code to said remote service provider.

4. The computer usable medium of claim **3** wherein said remote service provider examines the identification code in order to determine the number of times that the software has been activated on distinct user systems.

5. The computer usable medium of claim **4** wherein said number of times that said software has been activated on distinct user systems is updated each time that the activation code for such software is provided.

6. A method of protecting against software piracy, said method including the steps of:

a) configuring a software to enable it to receive an activation code for activating at least part of the functionality of said software;

b) distributing said software, said software requiring an activation code to activate at least part of the functionality thereof and wherein said software further has a unique identifier associated therewith to uniquely identify such software;

c) providing an activation code when the number of times that said software has been previously activated on distinct user systems in a manner that is independent of the identity of the user is less than a predetermined threshold, said predetermined threshold being at least two.

7. The method of claim **6** wherein said software is further configured to initiate contact with a remote service provider and to communicate said identification code to said remote service provider.

8. The method of claim **7** wherein said remote service provider examines the identification code in order to determine the number of times that said software has been activated on distinct user systems.

9. The method of claim **8** wherein said number of times that said software has been activated on distinct user systems is updated each time that the activation code for such software is provided.

10. A remote service provider comprising:

a) a data storage element that records the amount of activations for an authorized copy of software, wherein said amount of activations pertains to the number of times that the authorized copy of software has been activated, each authorized copy of software having an identification code associated therewith;

b) a processing element that examines the amount of activations recorded in the data storage element associated with an identification code in order to determine the number of times that the particular authorized copy of software associated with such identification code has been activated and wherein an activation code is provided for activating the authorized copy of software when the number of times that it has been previously activated on distinct user systems in a manner that is independent of the identity of the user is less than a predetermined threshold, said predetermined threshold being at least two.

11. The remote service provider of claim **10** wherein the processing element updates the amount of activations on distinct user systems recorded for an authorized copy of the software each time that the activation code for such authorized copy of the software is provided.

12. The remote service provider of claim **10**, wherein said activation code is provided by said processing element.

* * * * *