Softgoods Distribution Via A Network

Field of the invention

This invention relates to softgoods distribution via a network and refers particularly, though not exclusively, to softgoods distribution whereby the softgoods can be pre-installed prior to distribution.

Definitions

Throughout this specification a reference to softgoods is taken as including a reference to software as well as data.

Reference to related applications

Reference is made to earlier patent applications numbers PCT/SG99/00037 filed 10 march 1999, SG9903604-8 filed 24 July 1999, and SG9903866-3 filed 11 August 1999 (the "earlier applications"). The contents of the earlier applications are hereby incorporated by reference.

Background to the invention

Softgoods have traditionally been distributed on portable storage media, such as diskettes and CD-ROMs. The advent of networks such as the internet provided another distribution channel whereby softgoods could be downloaded on line, such as a customer downloading softgoods from a merchant. Both methods of distribution have significant shortcomings.

First, a customer is responsible for the installation of the softgoods. This may be a relatively non-trivial task for many people. Even with some popular installation methodologies used, the customer will often have to set the configuration from lengthy lists of options. Unless aware of the consequences of each possible choice, the customer

may be unwilling to proceed, or may make a decision which does not give the result the customer was hoping to achieve.

Secondly, there may be conflicts with other softgoods already installed, or in the process of being installed. Most computer users are incapable of, or not interested in, resolving such conflicts. This can impact on the sales or licensing potential of softgoods.

Thirdly, even after completing the installation of the softgoods, there may be maintenance work to be completed such as, for example, upgrading existing softgoods, applying patches, and so forth.

A significant problem is that the source of the softgoods, or the merchant supplying the softgoods, cannot ensure that the softgoods are used in accordance with the agreed terms upon which the softgoods were supplied to the customer. Once the customer has the softgoods they can repeatedly be installed, be shared with others, or duplicated not only in violation of the agreed terms but also in violation of intellectual property rights.

A number of merchants have recently commenced a service whereby customers can rent softgoods over the internet. By using such a service, a customer can run the supplied softgoods on the service provider's server using the internet to provide remote control. This allows the customer to use the softgoods without the problems and difficulties of installation and maintenance, and allows the merchant to retain control over the softgoods, the use of the softgoods, and so prevent unauthorized duplication.

However, since the softgoods always reside on the service provider's server all data and other information from the customer is sent over the internet from the customer to the service. If the data is sensitive, the customer may have reservations about entrusting the data to external parties. This is particularly so for corporate customers. Furthermore, the performance of such a service may be limited due to limited bandwidth, modem capabilities, the capacity of the customer's machine, and so forth. These problems have tended to limit the use of such services.

Consideration of Prior Art

There are three main categories of relevant prior art.

1. Online software rental and purchase. Those in this category pass software files to the client computer for execution - good for test-use and rental. In the case of software purchases, the software is installed permanently on the client computer. The technique used is basically drive mounting/mapping.

   These do not permit customization of software in test-use and rental modes, and software cannot be returned after purchase unless it is inherently faulty. They do not cover registry and environment setting issues during installation.

Internet online backup systems provide off-site remote storage for customers using various identification systems and passwords which were interactively established when signing.

US5,771,354

This specification discloses how a customer computer can connect to an online service provider computer by, phone, internet, or other method, pay a fee to the service provider, and obtain additional processing and storage resources for the customer's computer. The resources can take the form of storage and processing capabilities. These capabilities give the customer's computer what appears to be additional local processing power and/or additional local storage, this storage possibly including preloaded software and/or data. The additional resources made available to the customer computer can be used either to enhance the customers' local needs (such as access to storage for additional disk space, or access to a more powerful processor of similar type for program execution), or these additional resources can be used by the customer's computer's to support services on-line that otherwise would be unavailable, impractical, or unaffordable. Examples of services include software and information rental, sales, and release update services, anti-

viral services, backup and recovery services, and diagnostic and repair services, to name a few. However, with such systems all storage and relevant processing take place on the service provider's server. This requires all data from the customer to be transmitted to that server.

2. Metering/usage control after physically distributing part or all of software a user. Such systems do not address how to distribute the software or seamless switching between sales versus lease/rent/test-use, and so forth.

JP8,297,698 - COLLECTING METHOD FOR SOFTWARE RENT

In this specification, there is disclosed a system to suitably collect the rent of software by calling a substitutive information charge collection service in the case of performing an installation more than the prescribed number of times. When the installation on a hard disk device 5 is started by an instruction from a software user, a processor 1 firstly determines the number of times the software has already been installed by the user. This is recorded on a flexible disk 7 in accordance with a program for collecting the software rent. This calculates a value showing the current number of installations by adding 1 to the number of times it had been installed in the past. The processor 1 continually compares the number of times with a number representing the number of installations for which the software rent has been collected. When the number representing the number of installations for which rent has been collected is less than the number of installations, the software rent is collected by the substitutive information collection service.

JP8,044,451 - CHARGE CALL TYPE SOFTWARE RENT COLLECTING SYSTEM

The object stated in this specification is to provide a system to be used for the protection of the copyright of software and securing a copyright income. A software user is connected to a copyright manager through a communication system, e.g. a public line. Software to be distributed to each user is not complete. When the user tries to complete the software, the user's software automatically calls a copyright manager system. The manager system sends the required information for completing the user's system to the

user, through the communication service, and collects a software rent in response to the call.

CN1,152,841

This patent relates to a software protection method capable of making authorization automatic invalidation and particularly to a leased software protection method for a one-way propagation system including cable and satellite television, aerial, and so forth. The method can make the hirer of a software be unable to continuously use it after the expiry of the lease term of the software. When the authorization takes place, the time-signal sets of the hirer and the transmitter are synchronized. Depending on the broadcasting time of the software, the standard time signal of transmitter can be transferred to the hirer, and compared with the time at the hirer. If the difference between the time at the two ends exceeds a preset range, a control program is activated to stop the software.

US5,838,256

Relates to an electronic key with three modes of automatic self-disablement where there is provided an integrated circuit with three independently programmable "time bomb" functions. The integrated circuit can be set to disable itself after a certain number of power-up cycles, after a certain total duration of operation, or after a certain absolute time and date. This is particularly advantageous for authorization functions, where the manufacturer may want to enable the user to "test drive" a demonstration or rental item of hardware or software.

Further prior art documents include:

US5,870,726/WO.9,532,479 EP0,760,982

- protected software rental using smart cards;

EP0,895,148

- software rental system and method for rental software;

US5,715,169/EP0,671,711 CN1,117,622 JP7-244,781

- software rental method and apparatus, and circulating medium therefor;

JP8-007,009

- software rental system through network;

JP7-234,785

- computer and method for controlling rental period of software;

JP9-319,451

- rental fee determining device and use right managing device for computer software;

US5,649,187 US5,613,089, US5,497,479 US5,388,211 WO9,013,865

- method and apparatus for remotely controlling and monitoring the use of computer software;

US5,638,513 US5,548,645 US5,495,411 WO9,517,732 AU 14460/95

- secure software rental system using continuous asynchronous password verification; and

US5,925,127

- method and system for monitoring the use of rented software.

3. Creating user-modifiable view of internet sites

The disclosure below does not apply to softgoods in general. It also does not allow seamless switching between purchase versus lease/rent/test-use.

US5,889,951

Relates to systems, method, and computer program products for accessing, leasing, relocating, constructing and modifying internet sites within a multi-dimensional virtual reality environment.

This facilitates viewing, organizing, and optimizing internet sites. A multi-dimensional virtual environment includes one or more respective virtual sites for each internet site. Users are given the ability to explore the virtual environment and access internet site data and services via these virtual site(s). The transfer of data related to an internet site and its virtual site includes assigning a transfer priority to each virtual site based on the user's location within the virtual environment, and transferring data based on the assigned priority. Users are provided with the ability to lease portions of the virtual sites on leased portions, to assign internet site data and services to virtual sites, and to relocate virtual sites within the virtual environment.

Objects of the Invention

It is therefore the principal object of the present invention to provide softgoods distribution where the softgoods are installed on mobile computing environments, which can then be installed and run on a customer's machine.

A further object is to enable the terms of supply of the softgoods as agreed between the supplier of the softgoods and the customer prior to the supply of the softgoods, to be varied after the supply of the softgoods.

Summary of the invention

With the above and other objects in mind, the present invention provides a system for transferring softgoods from a sender to a recipient, the system including the steps of:

(a) the sender creating a mobile computing environment;

(b) the sender installing the softgoods on the mobile computing environment;

(c) transferring the mobile computing environment with the installed softgoods from the sender to the recipient such that upon the mobile computing environment being installed in a machine of the recipient the softgoods can be used by the recipient without the softgoods being installed on the recipient's machine;

(d) the transferring of the mobile computing environment with the installed softgoods being subject to terms relating to the use of the softgoods by the user, the terms being able to be varied subsequent to the installation of the mobile computing environment on the recipient's machine.

Preferably, the mobile computing environment is saved on a stable storage device for repeated uses. More preferably, the transference is by means of a network. The network may be the internet.

The recipient may obtain the softgoods for one or more modes of use including test use, evaluation, lease, rental, purchase. Preferably, the recipient can change from one mode of use to another after installation of the mobile computing environment. This may entail changing the licence under which the recipient uses the softgoods. Payment for the

softgoods by the recipient may be on a usage basis, at purchase, or on a time basis. Alternatively, the recipient can return the softgoods to the sender for an upgrade, refund or replacement.

More preferably, the terms may specify one or more of a period of time, an expiry date and time, or a predetermined number of uses, upon which event occurring the mobile computing environment is returned to the sender.

Advantageously, the recipient can add further softgoods to the mobile computer environment. More advantageously, the further softgoods remain on the recipient's machine and are able to be accessed by the recipient after the return of the mobile computing environment.

Preferably, the softgoods are encrypted with a sender secret key of the sender prior to their transference to the recipient. More preferably, the softgoods are decrypted using the sender secret key. Advantageously, the softgoods are re-encrypted after receipt by the recipient using a recipient secret key of the recipient.

Any further softgoods are encrypted with a further secret key of the recipient. Alternatively, the further softgoods are encrypted with a further recipient secret key of the recipient and a further sender secret key of the sender. The further softgoods may be decrypted using the further sender secret key.

Advantageously, the mobile computing environment obtains the sender secret key from the sender every time the recipient commences use of the softgoods.

More advantageously, the mobile computing environment and the sender authenticate each other before the sender releases the sender's sender secret key.

The mobile computing environment may be a virtual computer.

Description of the drawings

In order that the invention may be readily understood and put into practical effect, there shall now be described preferred embodiments of the present invention, the description being with reference to the accompanying illustrative drawings in which:

Figure 1 is a schematic flow chart of a preferred deployment architecture;

Figure 2 is a flow chart showing the steps used when softgoods are purchased; and

Figure 3 is a flow chart showing the steps used when softgoods are leased, rented or used on a trial basis.

Description of preferred embodiments

To first refer to Figures 1 and 2, there is shown a system architecture in which a network such as, for example, the internet is used. However, the present invention is not limited to use of the internet and use of a local area network, metropolitan area network, or other wide area network could be used. Also, physical networks such as "sneakernet" could also be used.

The sender (in this case a merchant) 1 has a machine 2 which is connected by network 3 to a merchant server 4. The merchant's sever 4 is connected to a recipient's (in this case a customer 7) server 5 again by the network 3. The network 3 may also connect the customer's server 5 to the customer's machine 6.

In the first step 8, the merchant 1 creates a virtual computer in his machine 2. The next step 9 in the process has the softgoods required by customer 7 to be installed onto the virtual computer by the merchant 1. The virtual computer with the installed softgoods is then saved on the merchant's server 4 (step 10) before being sent to the customer's server 5 via network 3 (step 11). The customer 7 can then load the virtual computer onto the customer's machine 6 from the customer's server 5, again via network

3 (step 12). The customer 7 can then use the virtual computer on the customer's machine 6 (step 13) in accordance with normal practices.

This is for a use mode where the customer 7 has purchased the softgoods from merchant 1. Such a purchase would be under normal, commercial terms and upon receipt of the softgoods the customer 7 is the owner thereof. However, as the softgoods are on a virtual computer within the customer's machine 6, they are not installed on the customer's machine 6. As such, they are installed in a virtual computer which, in turn, is installed on the customer's machine 6. Therefore, there is no difficulty of installation of the softgoods, and no patches are required for the softgoods to be able to be operated by customer 7 - the softgoods arrive in the customer's machine 6 ready to operate. In this regard, see the earlier applications.

If desired, the softgoods may be encrypted prior to being transmitted from the merchant's server 4 to the customer's server 5. Encryption may be by the virtual computer being given an identity prior to the softgoods being installed. A secret key is then generated by the merchant's server 4 and used to encrypt the softgoods.

Upon the virtual computer being downloaded to the customer's machine 6, the virtual computer establishes a connection with the merchant's server 4 via network 3. The connection may be a secure connection. Upon the connection being established, the virtual computer sends its identity to the merchant's server 4 via network 3, and the merchant's server 4 responds by sending to the customer's machine 6 the secret key to enable the softgoods to be decrypted. Such decryption is permanent, unless the customer re-encrypts the softgoods using a secret key of the customer.

Figure 3 is a flow chart for test-use/review/rental modes of use. The same procedure is used for all such use modes. As with the purchase use mode of Figure 2, the first step 14 is for the merchant 1 to load a clean virtual computer onto his machine 2.

In step 15, the merchant generates an identity and a secret key for that virtual computer. The merchant 1 then installs the softgoods for the customer 7 on the virtual

computer (step 16) and encrypts the softgoods using the secret key (step 17). The virtual computer with installed, encrypted softgoods is then saved at the merchant's server 4, and the identity and secret key are also saved at the merchant's server 4 (step 18). In step 19, the virtual computer with installed, encrypted softgoods is sent from the merchant's server 4 to the customer's server 5 via the network 3. The customer 7 can then load the virtual computer with installed, encrypted softgoods onto the customer's machine 6 (step 20).

The virtual computer then establishes a connection with the merchant's server 4 using network 3. This may be a secure connection. Upon the virtual computer establishing contact with the merchant's server, the virtual computer sends its identity to the merchant's server 4 via network 3. The merchant's server 4 then transmits the secret key to the virtual computer on the customer's machine 6 (step 21). The softgoods in the virtual computer are then decrypted by the virtual computer using the merchant's secret key (step 22) thus enabling the customer to use the softgoods in the normal manner (step 23).

Preferably, when the softgoods are no longer being used by the customer 7, the softgoods and the virtual computer are closed. Prior to closing, the softgoods are re-encrypted using the secret key. Therefore, every time the softgoods are to be used, the virtual computer must repeat steps 21 and 22. This enables the merchant 1 to not only maintain ownership over the softgoods, but also enables the merchant 1 to enforce those ownership rights, and to enforce the previously agreed terms under which the customer 7 obtained and uses the softgoods.

The customer 7 may add its own softgoods, including data, to the softgoods installed on the virtual computer. In this case, the customer retains ownership of such softgoods. However, they will be encrypted along with the softgoods of the merchant 1. To protect the customer 1, the customer's softgoods may be encrypted using a secret key of the customer 1, which can be obtained from the customer's key folder. Therefore, to use the softgoods, those supplied by the merchant 1 require the merchant's secret key obtained in the manner required by steps 21 and 22, and those supplied by the customer 7 require the customer's secret key.

Depending on the terms of the agreement between the merchant and the customer 7, upon the expiry of the agreement between them, the customer's softgoods installed on the virtual computer may be encrypted a final time but using the merchant's secret key as well as the customer's secret key so that the consent of both the merchant and the customer 7 is required for the customer's softgoods to be decrypted. The merchant's softgoods installed on the virtual computer will be encrypted using the merchant's secret key, as normal.

The terms of the agreement may specify that the customer's right of use of the merchant's softgoods installed on the virtual computer expire in any one or more of the following circumstances:

(a) a prescribed number of uses is reached;
(b) a preset expiry date is reached;
(c) a predetermined period of use expires; or
(d) payments from the customer 7 to the merchant 1 are not made as required.

Upon expiry due to those, or any other, reason (e.g. breach of other terms by the customer 1), the virtual computer and all of the installed, encrypted merchant's softgoods are returned to the merchant 1 at the merchant's server 4.

Alternatively, if as a result of the trial use/test use/rental, the customer 7 wants to change the mode of use of the softgoods, eg, purchase, upon agreement with the merchant 1 being reached, and the commercial requirements of the merchant 1 being satisfied, the merchant's secret key is sent by the merchant's server 4 to the virtual computer to decrypt the softgoods, whereupon the softgoods are re-encrypted using the customer's secret key. The customer can then use the softgoods in the normal manner. If the change in mode of use is from test use to rental, the softgoods remain encrypted with the merchant's secret key, as is described above.

As the virtual computer can run on a different machine from the merchant's server 4 and the customer's machine 6, one or both of their secret keys may need to be sent over the network 3 to the virtual computer. To protect the secret keys from each other, and from third parties, the merchant 1, the customer 7, and the virtual computer may each have a pair of public and private keys, which are preferably generated in accordance with the RSA public-key cryptography system. When the merchant 1 generates the virtual computer in step 14, and the secret keys are created in step 15, the public key of the merchant 1 is embedded in the virtual computer, and the merchant's server 4 stores a copy of the virtual computer's public key. This enables the merchant's server 4 and the virtual computer to authenticate each other before the merchant's server 4 releases the secret key to the virtual computer, preferably over a secure channel in network 3.

The protocol for authentication and securing the transmission channel is based on the standard Secure Socket Layer (SSL) protocol. Likewise, the customer's secret key is released to the virtual computer using the SSL protocol.

Whilst there has been described in the foregoing description preferred embodiments of softgoods distribution via a network, it will be understood by those skilled in the art that many variations or modifications may be made without departing from the present invention.

The claims:

1. A system for transferring softgoods from a sender to a recipient, the system including the steps of:

(a) the sender creating a mobile computing environment;

(b) the sender installing the softgoods on the mobile computing environment;

(c) transferring the mobile computing environment with the installed softgoods from the sender to the recipients such that upon the mobile computing environment being installed in a machine of the recipient the softgoods can be used by the recipient without the softgoods being installed on the recipient's machine;

(d) the transferring of the mobile computing environment with the installed softgoods being subject to terms relating to the use of the softgoods by the user, the terms being able to be varied subsequent to the installation of the mobile computing environment on the recipient's machine.

2. A system as claimed in claim 1, wherein the mobile computing environment is saved on a stable storage device for repeated uses.

3. A system as claimed in claim 1 or claim 2, wherein the transference is by means of a network.

4. A system as claimed in claim 3, wherein the network is the internet.

5. A system as claimed in any one of claims 1 to 4, wherein the recipient obtains the softgoods for one or more modes of use including test use, evaluation, lease, rental, purchase.

6. A system as claimed in claim 5, wherein the recipient can change from one mode of use to another after installation of the mobile computing environment.

7. A system as claimed in claim 6, wherein the change in mode of use entails changing the licence under which the recipient uses the softgoods.

8. A system as claimed in any one of claims 1 to 7, wherein payment for the softgoods by the recipient is to be on a usage basis, at purchase, or on a time basis.

9. A system claimed in any one of claims 1 to 7, wherein the recipient can return the softgoods to the sender for an upgrade, refund or replacement.

10. A system as claimed in any one of claims 1 to 7, wherein the terms specify one or more of a period of time, an expiry date and time, or a predetermined number of uses upon which event occurring the mobile computing environment is returned to the sender.

11. A system as claimed in any one of claims 1 to 10, wherein the recipient can add further softgoods to the mobile computer environment.

12. A system as claimed in claim 11, wherein the further softgoods remain on the recipient's machine and are able to be accessed by the recipient after the return of the mobile computing environment.

13. A system as claimed in any one of claims 1 to 13, wherein the softgoods are encrypted with a sender secret key of the sender prior to their transference to the recipient.

14. A system as claimed in claim 13, wherein the softgoods are decrypted using the secret key.

15. A system as claimed in claim 14, wherein the softgoods are re-encrypted after receipt by the recipient using a recipient secret key of the recipient.

16. A system as claimed in any one of claims 13 to 15, wherein any further softgoods are encrypted with a further secret key of the recipient.

17. A system as claimed in any one of claims 13 to 15, wherein the further softgoods are encrypted with a further recipient secret key of the recipient and a further sender secret key of the sender.

18. A system as claimed in any one of claims 13 to 17, wherein the further softgoods may be decrypted using the further sender secret key.

19. A system as claimed in any one of claims 13 to 18, wherein the mobile computing environment obtains the sender secret key from the sender every time the recipient commences use of the softgoods.

20. A system as claimed in any one of claims 13 to 19, wherein the mobile computing environment and the sender authenticate each other before the sender releases the sender's sender secret key.

21. A system as claimed in any one of claims 1 to 20, wherein the mobile computing environment is a virtual computer.