PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 3 :
H04L 9/00, G01F 1/00
G06K 5/00, G06F 13/06

A1

(11) International Publication Number: **WO 85/ 02310**

(43) International Publication Date: 23 May 1985 (23.05.85)

(21) International Application Number: PCT/US84/01856

(22) International Filing Date: 14 November 1984 (14.11.84)

(31) Priority Application Number: 551,125

(32) Priority Date: 14 November 1983 (14.11.83)

(33) Priority Country: US

(71) Applicant: SOFTNET, INCORPORATED [US/US]; 53 Dean Road, Weston, MA 02193 (US).

(72) Inventors: HANSCHE, Lance, E. ; 53 Dean Road, Weston, MA 02193 (US). COLVIN, Neil, J. ; 1 Knollwood Street, North Easton, MA 02356 (US).

(74) Agent: HENNESSEY, Gilbert, H.; Kenway & Jenney, 60 State Street, Boston, MA 02109 (US).

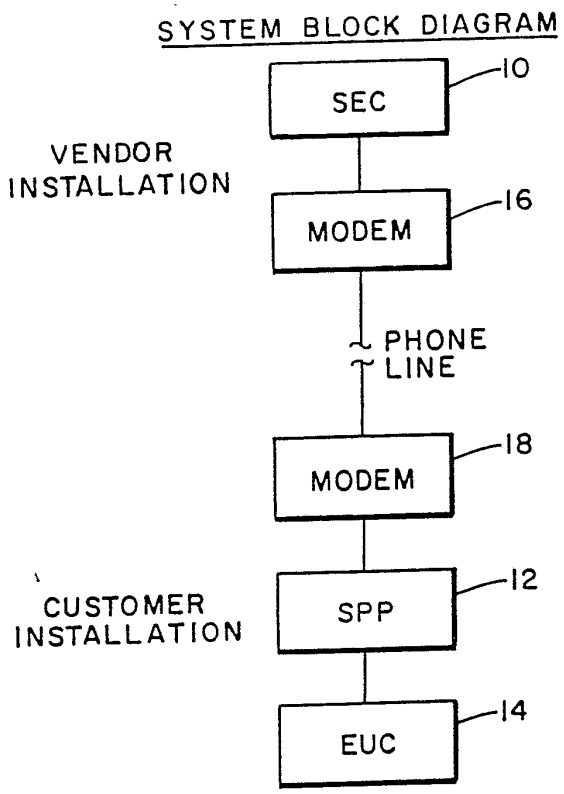
(81) Designated States: BE (European patent), DE (European patent), FR (European patent), JP, SE (European patent).

Published
With international search report.

(54) Title: SOFTWARE DISTRIBUTION SYSTEM

(57) Abstract

A system for distributing copies of computer software provides inherent protection against unauthorized copy of the software. The software distribution system includes three computers: a host (10), a software protection computer (12) and an end-user computer (14). The host computer (10) is under the control of the vendor, and the software protection computer (12) and the end-user computer (14) are located at the customer installation. The software is encrypted in the host computer (10) and then transferred to and stored in the end-user computer (14) after it is registered in the software protection computer (12). The transferred software is encrypted using a unique encryption key. Each copy of a software package generated by the host computer (10) is a unique encrypted version of that software package. When this unique encrypted version of the software package is run on the end user's computer (14) and encounters an encrypted portion of itself, it will suspend normal execution and transfer the encrypted portion to the software protection computer (12). This computer (12) will then decrypt the encrypted portions of the code and return the decrypted portion of the code to the end-user computer (14) where that code is itself executed or allows execution of the program of which it is a part to continue.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BG	Bulgaria
BR	Brazil
CF	Central African Republic
CG	Congo
CH	Switzerland
CM	Cameroon
DE	Germany, Federal Republic of
DK	Denmark
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
HU	Hungary
IT	Italy
JP	Japan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
MC	Monaco
MG	Madagascar
ML	Mali
MR	Mauritania
MW	Malawi
NL	Netherlands
NO	Norway
RO	Romania
SD	Sudan
SE	Sweden
SN	Senegal
SU	Soviet Union
TD	Chad
TG	Togo
US	United States of America

SOFTWARE DISTRIBUTION SYSTEM

BACKGROUND OF THE INVENTION

This invention relates to electronic software distribution and more particularly to a software distribution system in which the distributed software is protected against copying.

Over the past few years, the growth of the software industry has been enormous, and as more and more people purchase personal computers, the industry is expected to continue to grow rapidly. For the most part, purchased software changes hands from a mail order or retail vendor to a customer in some physical form such as a tape, disk or even a printed listing of code. Such physical distribution has resulted in a number of problems with respect to both the mode of distribution and customer servicing as well as with the rights of the creators and publishers of the software which is sold. Principal among the problems is that a large percentage of the software which is sold ends up being illegally copied. Frequently, a purchaser of software will "lend" his copy of the software to a friend who makes a copy for himself. The most obvious result of this unauthorized copying is that the profits of the creator and publisher of the software (who probably have a copyright in the software) are greatly reduced. To make up for these lost profits, the price of the software is maintained at a high level. This sustained high price unfortunately produces an even greater incentive to illegally copy.

Copyright protection, which does provide the creator and publisher of software with legal recourse against the person making the unauthorized copies has, in fact, afforded little or no relief from the problem of copied software. As the copies are often made by individuals for their own use, large-scale policing

of such copying is virtually impossible. On rare occasions, a copier having a large copy resale operation can be caught, but by the time he is caught, many unprotected copies usually already have been distributed. Furthermore, the advent of software rental shops has further limited the copyright owner's ability to protect his rights in the software he owns.

Another problem frequently encountered with software sold over the counter is the need to later distribute revised copies to add new features or to fix errors or "bugs" present in the software. These bugs appear despite rather substantial testing that is performed before a software package is put on the market. These bugs are particularly prevalent in software which has recently entered the market. In order to correct any errors which do appear in the software, a software publisher must recall the disk or tape which contains the faulty software. The problem with correcting errors in this manner is that the software is out of the hands of the purchaser for a number of days, if not weeks, while the exchange and correction take place. Finally, the cumbersome nature of this system discourages the user's updating of his software which often leaves a bad impression of the software publisher's products in the field.

In order to combat the illegal copying of software, the software industry has taken a number of precautions. The various approaches fall under three categories: media protection against copying, use of read-only media and processor serialization.

Media protection against copying refers to making some unique version of the medium containing the software. One type of media protection involves the use of variable-pattern diskettes. Variable-pattern diskettes, however, do not offer a practical solution to the software copying problem since these diskettes depend on a soft format diskette drive and they are

vulnerable to memory copy if the entire program is loaded at once. Furthermore, such variable-pattern diskettes can only be used in a small percentage of the drives currently on the market. Therefore, the software distributed on such diskettes can only be offered to a rather small percentage of the market. Finally, physical alteration of the media, usually by forcing hard errors on the media checked for by the software itself, has been used. This method fails in that hardware checks in the software can be located and neutralized in the software itself.

Another type of media protection against copying involves the use of an operating system override. Such a protection scheme depends on a rather unique operating system which prevents copying of diskettes. The use of an operating system override, however, has not proven to be the answer to the problem either since the altered operating system must be tailored to the particular controller chip of the computer on which it is operating, and the operating system override cannot support use with standard operating systems currently on the market. In addition, any operating system override is vulnerable to an algorithmic solution or "cracking". One variation on the operating system override scheme has the software employ features of the hardware, circumventing the operating system, to check areas on the storage media which the operating system cannot reach. This method can also be defeated by being neutralized in the software itself.

A third type of media protection against copying involves the use of segmented programs in conjunction with variable-pattern diskettes and/or an operating system override. The use of such segmented programs of necessity requires some type of a segment loader to read in the various segments when required. This results in very slow response from a computer utilizing such segmented programs. Furthermore, any loader

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.